Fall 2013

The impact of organizational insiders' psychological capital on information security

A. J. Burns III

THE IMPACT OF ORGANIZATIONAL INSIDERS' PSYCHOLOGICAL CAPITAL ON INFORMATION SECURITY

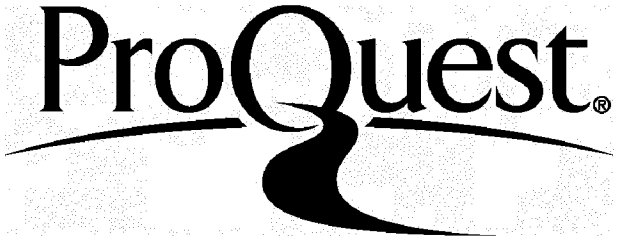
by

A. J. Burns, III, B.S., M.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

November 2013



LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

August 8, 2013

Date

We hereby recommend that the dissertation prepared under our supervision by A. J. Burns

entitled The Impact of Organizational Insiders' Psychological Capital on Information Security

be accepted in partial fulfillment of the requirements for the Degree of Doctor of Business Administration

Supervisor of Dissertation Research

Head of Department

Accounting & Information Systems

Department

Recommendation concurred in:

Advisory Committee

Approved:

Director of Graduate Studies

Approved:

Dean of the Graduate School

Dean of the College

GS Form 13a
(6/07)

ABSTRACT

This dissertation research seeks to examine the role of organizational insiders' psychological capital (PsyCap) on the performance of protection motivated behaviors (PMBs). The dissertation examines the role of PsyCap through three studies which were conducted for this research. Using structural equation modeling (SEM), the responses from four distinct samples were analyzed. The results largely support the significant role of PsyCap in information security. The first study takes an expectancy theory (Vroom, 1964) approach and found that PsyCap was a significant consequence of insiders' security-related expectancy dimensions. Additionally, expectancy theory was found to be an appropriate frame-work for promoting PMBs.

The expectancy dimensions were found to be trainable through security, education, training, and awareness (SETA) programs, and were significantly related to the performance of PMBs. The second study draws upon the broaden-and-build theory (Fredrickson, 2004) to examine the role of PsyCap within an emotional security framework. The second study found that the broaden-and-build theory explained the performance of PMBs through a direct relationship between emotion and behavior as well as through an indirect relationship between emotions and an insider's PsyCap.

Finally, the dissertation examines the role of PsyCap in information security from a framework of behavioral complexity (Wu et al., 2010) in the third study. The results of the third study indicate that PsyCap is a significant contributor to a model of security

behavioral complexity which is shown to effectively influence insiders' performance of PMBs. Implications of the results on both practice and research are discussed along with limitations to the current studies. The overall contributions of the dissertation are highlighted and areas of future research evidenced by the findings are raised.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author 

Date 8-8-2013

GS Form 14
(5/03)

DEDICATION

To my family.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

I would like to acknowledge the support of my committee members: Dr. Tom Roberts and Dr. Jim Courtney, dissertation co-chairs, along with Dr. Rebecca Bennett and Dr. Clay Posey. This work is an artifact of their guidance and support. I am fortunate to count these as mentors, colleagues, and friends. I am thankful to the faculty, staff, and fellow students of Louisiana Tech University for the important role each has played in this process as well.

CHAPTER 1

INTRODUCTION

In today's knowledge economy, organizational success is increasingly reliant upon the effective utilization of organizational information systems (IS). In order to leverage the capabilities enabled by new technology, organizations often provide employees with access to information and information systems on an ongoing basis. This increased access provided by enterprise-wide systems and ubiquitous computing exposes the organization's systems to risks beyond the proximate control of the IT staff (Vroom et al., 2004). Given this complexity, it is not an understatement to say that the organization's resources and systems are largely at the mercy of the actions of all insiders with access to the IS (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; D'Arcy & Hovav, 2007; Moore, Cappelli, & Trzeciak, 2008). In fact, According to a recent survey of security practitioners, the complexity of the security environment, not a lack of resources was the most widely reported cause of information security concerns (Richardson, 2010/2011).

The reliance upon the behavior of employees for organizational information security led to the genesis of a branch of information security research deemed behavioral information security. B*ehavioral information security* is defined as the study of "the human actions that influence the availability, confidentiality, and integrity of information systems" (Stanton et al., 2006b, p. 263). To date, most research into behavioral

information security has been in line with the perspective that users are generally bad actors, and any increase in user computing ability can be associated with an increased threat to the organization (Straub et al., 1990; Zafar et al., 2009). Recently, however, it has become known that many organizational insiders have requisite knowledge and ability to affect organizational security positively through their use of and interactions with technology and information systems in the workplace (Posey et al., 2013). *Organizational insiders* are all individuals (e.g., full- and part-time employees, temporary workers, board members) who have access to organizationally relevant information while fulfilling their duties (Posey et al., 2013; Shaw et al., 1998). The volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS in which that information is stored, collected, disseminated, and/or manipulated from information-security threats are protection-motivated behaviors (PMBs) (Posey et al., 2013).

The shift of behavioral information security to consider the security abilities of the average employee has mirrored a similar shift in psychology brought about by the positive psychology movement (Seligman et al., 2000). Positive psychology is "the study of the conditions and processes that contribute to the flourishing or optimal functioning of people, groups, and institutions" (Gable et al., 2005). Drawing on positive psychology, this dissertation extends the body of knowledge in behavioral information security by considering the impact of employees' psychological capital (PsyCap) on the security-related outcomes of an organization. *PsyCap is* a higher order construct made up of core tenets of positive psychology conceptualized as hope, self-efficacy, resilience, and optimism (Luthans et al., 2007a).

Psychological Capital

As a higher-order construct, PsyCap is composed of distinct yet related core tenets of positive psychology of hope, resilience, optimism, and self-efficacy. P*ositive psychology* is interested in "optimal functioning" or what is referred to in its literature as "flourishing" (Seligman et al., 2000). A key characteristic of positive psychology that makes it an ideal candidate for consideration in behavioral information security—especially dealing with the security behaviors of insiders—is that it is a branch of traditional psychology that has the "average person" as its subject (Sheldon et al., 2001). Therefore, positive psychology is fertile ground for the cultivation of appropriate security behaviors of ordinary organizational insiders, and PsyCap provides a succinct and well-established construct for investigating the role of positive psychology in information security. The four subconstructs of PsyCap are described next and are summarized in Table 1.1.

PsyCap hope is a "positive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287; Luthans et al., 2007a). *PsyCap resilience* "is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans et al., 2007a, p. 546; Masten, 2001; Masten et al., 2002). Resilience can also be thought of simply as "the positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702; Luthans et al., 2007a). *PsyCap optimism* is the characteristic of individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them" (Scheier et

al., 1985). *PsyCap self-efficacy* is a role-breadth self-efficacy and is defined as "the employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66; Luthans et al., 2007a).

Table 1.1

Summary of PsyCap Characteristics

PsyCap Component	Definition	Micro-Development
PsyCap Self-Efficacy	"[T]he employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66)	• Mastery experiences • Modeling and vicarious learning • Social persuasion • Physiological and psychological arousal
PsyCap Hope	"[P]ositive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287).	• Goal-setting • Participation • Contingency planning for alternative pathways to attain goals
PsyCap Optimism	Characterizes individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985).	• Leniency for the past • Appreciation for the present • Opportunity-seeking for the future
PsyCap Resilience	"[T]he positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702)	• Asset-focused strategies such as enhancing employability • Risk-focused strategies such as proactive avoidance of adversity • Process-focused strategies to influence the interpretation of adverse events
Adapted from descriptions in *Psychological capital: Developing the human competitive edge,* Luthans, Youssef, et al. (2007b).		

Though a relatively new construct, PsyCap, has already been widely accepted and used extensively in the field of organizational behavior and beyond (Avey et al., 2009;

Walumbwa et al., 2011; Avey et al., 2010; Peterson et al., 2011; Abbas et al., 2012; Wang et al., 2012). One reason that PsyCap has been so widely used is that it has been shown to be composed of characteristics that are state-like rather than trait-like. Though research has often relied on context to inform the true distinction between state and trait (Allen et al., 1981), an important distinction can be made between trait-like and state-like dispositions (Zuckerman, 1983; Fugate et al., 2012). This differentiation is especially critical in a security context because PsyCap, a construct composed of state-like characteristic, has been shown to be developable (Luthans et al., 2007a; Luthans et al., 2006a; Peterson et al., 2011). Therefore, any benefits to firm security that can be shown to be attributable to PsyCap can be influenced by an organization through what could be thought of as an investment in employees' PsyCap.

Additionally, malleability is an important criterion for inclusion into behavioral information security. To fully recognize the potential benefits of considering PsyCap in behavioral information security, the methods for developing PsyCap should also be considered. As PsyCap is a latent construct composed of four underlying characteristics, it can be developed at the facet level by developing each of the individual characteristics (Luthans et al., 2006b; Luthans et al., 2006a). A thorough treatment of PsyCap "micro-intervention" can be found in Luthans et al. (2007b), and is summarized in Table 1.1. PsyCap is a higher-order reflective construct, which means that the facets of PsyCap vary together (Jarvis et al., 2003; Bagozzi, 2011). Building PsyCap at the facet level should take advantage of the reported synergistic relationship among the indicators and lead to an increase in the overall PsyCap construct (Luthans et al., 2007b).

As the name implies, PsyCap can be thought of quite literally as a factor of psychological production. In parallel to the traditional factors of economic production, land (or natural resources), labor, and capital (Beer, 1980; Huettner et al., 1982), PsyCap meets the criteria of a psychological resource (Avey et al., 2009). PsyCap can therefore be viewed through the lens of resource theory (Luthans et al., 2007b; Hobfoll, 1989; Hobfoll, 2002). Hobfoll's (1989) describes the role of resources, stipulating that individuals require resources for functioning, and they will seek to gain available resources and when possible conserve unnecessarily expended resources. Thus, the conservation of resources has two components: the building of resources and the conservation of resources. PsyCap as a resource can be built by either micro-intervention (see Table 1.1) or by macro-intervention such as a supportive climate (Luthans et al., 2008). In reference to conservation, resources are either "centrally valued in their own right" or "as a means to obtain centrally valued ends" (Hobfoll, 2002). PsyCap can be viewed as adaptive in that not only does PsyCap embody a positive psychological state, as a psychological construct it serves meaningful ends. For instance, PsyCap has been shown to provide a necessary psychological resource for psychological well-being (Culbertson et al., 2010).

Theoretical Foundation of Dissertation

This dissertation includes three studies which each examine a novel and unique approach to behavioral information security. As implied in the name of the tome, common to the studies is an examination of the role of insider's PsyCap. The first study is grounded in expectancy theory (Vroom, 1964) and simultaneously assesses the responsiveness of expectancy dimensions to training and the impact of expectancy

dimensions on motivation to and withdrawal from protective security behaviors. The second study examines the impact of emotion in information security and is grounded in the broaden-and-build theory (Fredrickson, 2004). The final study develops and examines a model of security behavioral complexity (Wu et al., 2010), consisting of security behavioral repertoire, security differentiation, and PsyCap. The succeeding sections provide a brief articulation of the theoretical foundation of each of the three security studies including PsyCap.

Study 1: A Multi-Dimensional Assessment of Organizational Insiders' Performance of Protection-Motivated Behaviors: An Expectancy Theory Approach

Originally developed by Vroom (1964), expectancy theory has been used in numerous studies involving motivation in the workplace (Van Eerde et al., 1996). Expectancy theory enables a multidimensional diagnostic approach to motivation (Sanchez et al., 2000; Ilgen et al., 1981; Courtney et al., 1983; DeSanctis, 1983). Expectancy theory—also referred to as VIE theory—offers a set of three motivational antecedents consisting of (1) valence, (2) instrumentality, and (3) expectancy (Ellingson et al., 2011). *Valence* is the preference of one outcome over another (or all others) (Vroom, 1964). *Instrumentality* is an individual's perception that successfully enacting a behavior will lead to an ultimate outcome (Vroom, 1964). *Expectancy* is an "action-outcome association" and is defined as is a perception that an individual's efforts will lead to the intended behavior (Vroom, 1964).

This study explores the impact of expectancy measures on insiders' motivation to and withdrawal from performance of PMBs. In addition to the direct effect of expectancy measures, it also explores antecedents and consequences of expectancies. First the impact

of security education, training and awareness (SETA) on expectancy dimensions is assessed. *SETA* programs are the mechanism by which organizations inform users of security threats, establish the responsibilities of the employees, and detail the consequences of failing to comply (D'Arcy et al., 2009; Straub et al., 1998). Finally, the impact of expectancies on insiders' PsyCap in addition to the role of PsyCap in the motivation to and withdrawal from PMBs is assessed. The research model for the expectancy theory study is shown in Figure 1.1.

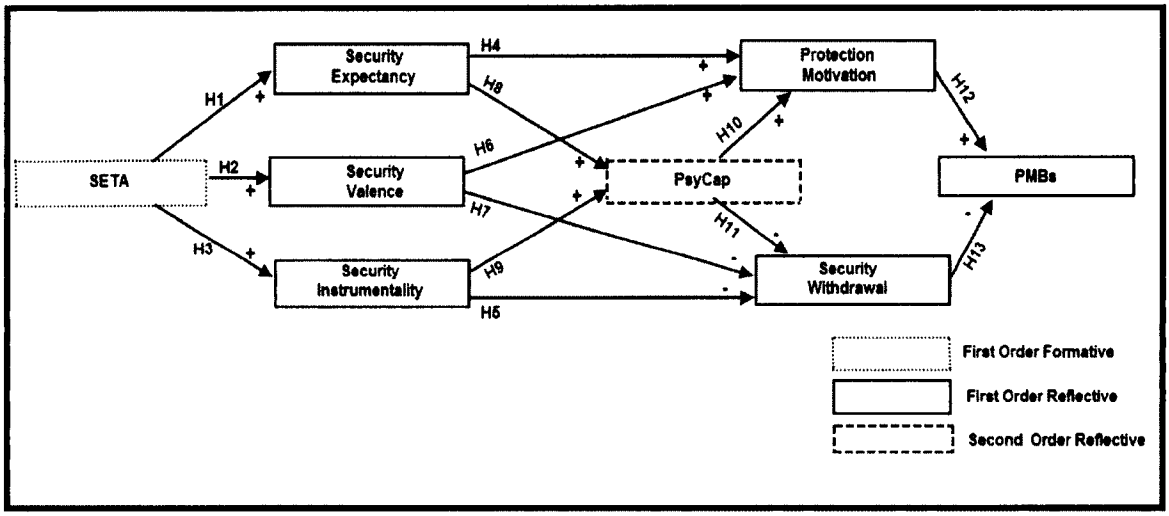


Figure.1.1 *Chapter 1 Research Model*

Study 2: The Adaptive Role of Emotion in Information Security: Broadening the Theoretical Repertoire

As in the broader organizational literature (Fredrickson, 1998), where the IS security literature has considered emotions at all, it has most often considered the role of negative emotions such as fear (e.g. Johnston et al., 2010). However, emotional stimuli often elicit multiple emotions of varying intensities simultaneously (Lazarus et al., 1984; Lazarus, 1991; Beaudry et al., 2010). The broaden-and-build theory (Fredrickson, 1998; Fredrickson, 2001) provides a multi-dimensional framework of emotions which includes

the often neglected positive emotions. The *broaden-and-build theory* posits that positive emotions "broaden the scope of attention and thought-action repertoires," (Fredrickson et al., 2005) while simultaneously building lasting psychological resources (Fredrickson, 1998; Fredrickson, 2001; Fredrickson et al., 2005). An individual's *thought-action repertoire* is the collection of the thoughts and behaviors which are cognitively available in the moment of action (Fredrickson et al., 2005).

Organizations often play on the emotions of employees to elicit security behaviors by employing appeals to emotion, such as fear (Johnston et al., 2010; Anderson et al., 2010; Herath et al., 2009; Lee et al., 2009). Yet, as the role of emotion becomes increasingly important in IS (Beaudry et al., 2010), even the established role of fear has been called into question (Crossler et al., 2012). The broaden-and-build theory explains that certain emotional responses to security threats (i.e. emotions such as fear and anxiety) may have a confounding effect on proactive security behaviors such as PMBs (Fredrickson, 2001). The goal of this study is to integrate a framework of emotions (Beaudry et al., 2010) with the broaden-and-build theory (Fredrickson, 1998, 2001) in order to examine the adaptive role of emotions in information security. The research model for the Chapter 2 is shown in Figure 1.2.

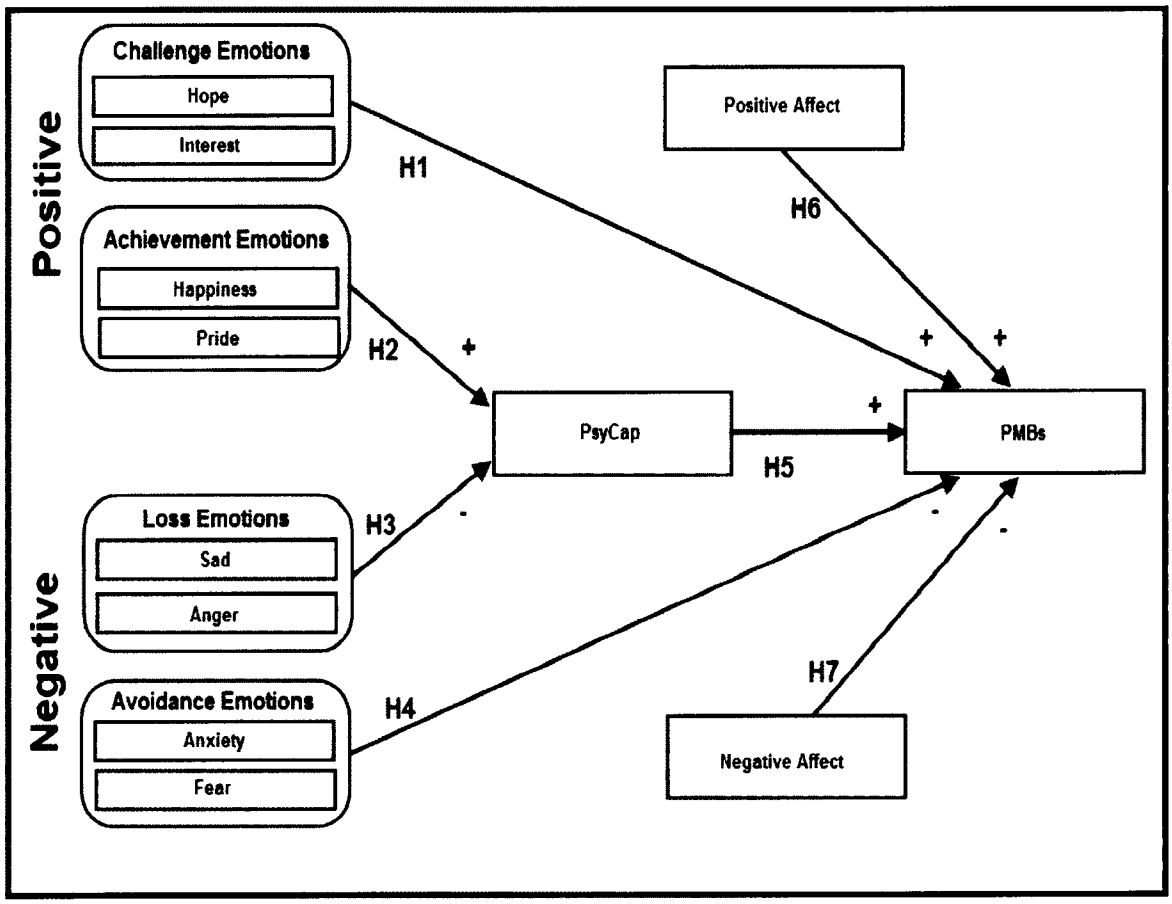


Figure 1.2 *Chapter 2 Research Model*

Study 3: Security Behavioral Complexity and Psychological Capital: An Empirical Examination

The protective roles (e.g. PMBs) which insiders may enact in order to protect the firm's information and IS may be unrelated to or even in direct contrast with an insider's formal job description. In this way, PMBs are enacted alongside the various organizational roles held by all insiders with access to informational resources, creating behavioral complexity for insiders (Posey et al., 2013). *Behavioral complexity* refers to "the ability to act and play multiple roles that call for diverse and even competing behaviors" (Wu et al., 2010, p. 818). Hooijberg (1996) established that behavioral complexity is comprised of two distinct components: (1) behavioral repertoire and (2) behavioral differentiation. *Behavioral repertoire* is the portfolio of roles an individual

performs and his or her ability to perform multiple roles, and *behavioral differentiation* is the ability to "switch from role to role at appropriate times to handle paradoxes and contradictions mandated by one's job" (Wu et al., 2010, p. 818).

Insiders' PMB complexity has recently been espoused as an antecedent to the performance of PMBs (Posey et al., 2013), but has yet to be empirically examined. Complementary to behavioral complexity are personal resources such as PsyCap which equip an individual to deal with the tensions of divergent demands (Smith et al., 2011). This study reports an empirical examination of a model of behavioral security complexity, which considers the impact of PMB complexity and PsyCap simultaneously. The research model for the Chapter 3 study is shown in Figure 1.3.

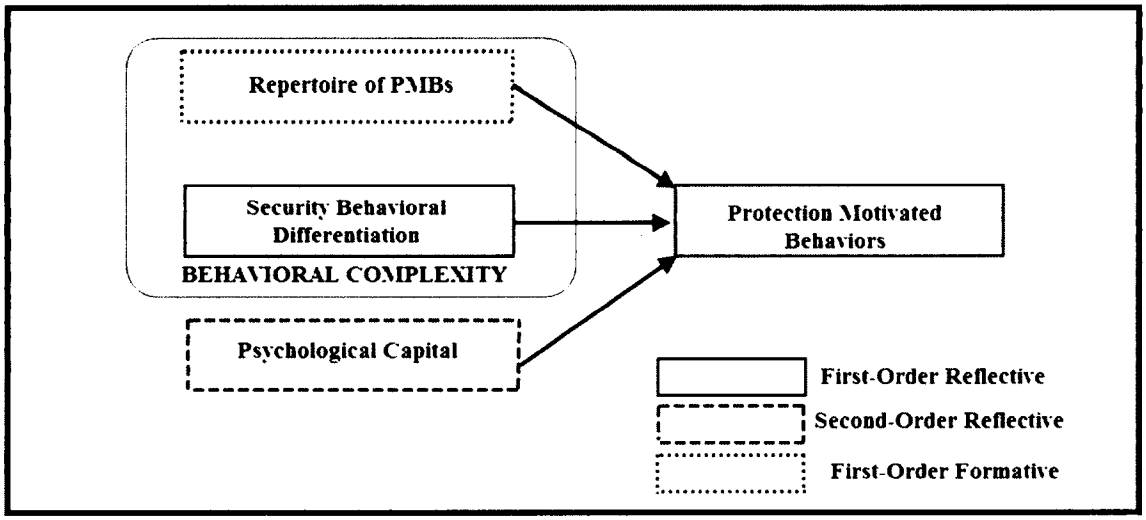


Figure 1.3 *Chapter 3 Research Model*

The remainder of the work is dedicated to the development and empirical examination of the three studies outlined in this chapter. Each study is self-contained within its own chapter (chapters two, three, and four, respectively). The final chapter of the dissertation, chapter five, concludes the work with a summary of the findings.

CHAPTER 2

A MULTI-DIMENSIONAL ASSESSMENT OF ORGANIZATIONAL INSIDERS' PERFORMANCE OF PROTECTION-MOTIVATED BEHAVIORS: AN EXPECTANCY THEORY APPROACH

Introduction

In today's technology-driven economic environment, many employees have unprecedented access to their organizations' information and information system (IS), (Dhillon et al., 2001; Zafar et al., 2009; Stanton et al., 2006b; Stanton et al., 2006a). This increased access provided by enterprise-wide systems and ubiquitous computing often exposes the organization's systems to risks beyond the proximate control of the IT staff (Vroom et al., 2004). It is increasingly difficult for organizations to maintain information security, as 54% of firms report an inability to determine if off-site employees are using technology and informational resources within corporate and regulatory requirements (Ponemon, 2013). These realities have led many practitioners and academicians to recognize that organizational information security is at the mercy of the actions of those with access to the firm's information and IS (Moore et al., 2008; Boss et al., 2009; D'Arcy et al., 2007).

The study of "the human actions that influence the availability, confidentiality, and integrity of information systems" is *behavioral information security* (Stanton et al.,

2006b, p. 263). Behavioral information security research examines the impact of organizational insiders' behavior on information security—often in order to assess or deter the diminution of security brought on by insider behavior (e.g. Shaw et al., 1998; Boss et al., 2009; Vroom et al., 2004; Willison et al., 2009; Greitzer et al., 2008; Zafar et al., 2009; Straub et al., 1990; Sasse et al., 2001). *Organizational insiders* are individuals (e.g., full- and part-time employees, temporary workers, board members) who have access to organizationally relevant information while fulfilling their duties (Posey et al., 2013; Shaw et al., 1998). However, just as insiders may jeopardize information security by behaving maliciously (e.g. Straub et al., 1990; Posey et al., 2011; Whitman, 2003) or carelessly (e.g. Johnson, 2008; Workman et al., 2008; Im et al., 2005), insiders who actively and conscientiously work toward the protection of the firm are able to increase information security (Posey et al., 2013; Albrechtsen et al., 2009; Stanton et al., 2005).

Posey et al. (2013) comprehensively identified many of the security-enhancing behaviors an insider can perform by developing a taxonomy of protection-motivated behaviors (PMBs) . *PMBs* are the volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS in which that information is stored, collected, disseminated, and/or manipulated from information-security threats (Posey et al., 2013). PMBs include a broad swath of protective behaviors ranging from maintaining general security etiquette to identifying and reporting suspicious co-worker behavior (Posey et al., 2013). Therefore, in addition to deterring the harmful behavior of some corrupted and/or heedless employees, effective security requires that organizations motivate insiders to reach their protective potential through the performance of PMBs.

To examine insiders' motivation to perform PMBs, I employ a multi-dimensional model of motivation grounded in expectancy theory (Vroom, 1964). *Expectancy theory* is a behavioral process theory (Brouer et al., 2011), which explains motivation as a product of both individual preferences and perceptions of outcome probabilities (Vroom, 1964). This essay evaluates the impact of expectancy measures on insiders' motivation to and withdrawal from performance of PMBs. In addition, to more fully explicate the role of expectancy theory in eliciting protective behaviors, this research includes key antecedents and consequences to the expectancy measures as well. First, the role of security education, training and awareness (SETA) is examined as an antecedent to expectancy theory. *SETA* programs are the mechanism by which organizations inform users of security threats, establish the responsibilities of employees, and detail the consequences of failing to comply (D'Arcy et al., 2009; Straub et al., 1998). Second, the role of expectancy theory in building insiders' psychological capital (PsyCap) is analyzed. *PsyCap* is a higher order construct conceptualized as hope, self-efficacy, resilience, and optimism (Luthans et al., 2007a) that has emerged out of the positive psychology movement (e.g. Seligman et al., 2000).

Background

Driving the importance of information security is a realization that protection of information resources is paramount for organizational success and should be a primary goal of the organization (Siponen et al., 2010; Herath et al., 2009; Dhillon et al., 2006). Information security has most often placed primary focus on technical methods and managerial approaches to safeguard against security-threatening behavior (Zafar et al., 2009; Choobineh et al., 2007). PMBs, however, imply a broadened view of the insider

from merely a threat to a potential protector of information security (Posey et al., 2013; Albrechtsen et al., 2009; Stanton et al., 2005).

Organizations seeking to motivate employees to protect the organization tend to focus on employees' compliance with formalized security policies (Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath et al., 2009; Vroom et al., 2004). Security policy compliance is an important goal for any organization, without which the policy itself is meaningless (Siponen, 2000). Yet security policy compliance represents only one subset of the protective behaviors in which an insider can engage (Posey et al., 2013; Albrechtsen et al., 2009). Additionally, policies are often constructed with a negative frame, such that they generally focus on telling employees what not to do to deter unwanted behavior such as computer abuse rather than telling employees what to do to protect the organization (Lee et al., 2002). Security research has also investigated individuals' intentions to adopt software solutions such as anti-malware software (Lee et al., 2009) or anti-spyware software (Johnston et al., 2010). These software solutions are important safeguards; however, they are most often adopted by the IT department and represent an organization's investment in IT security rather than the motivation of insiders' to protect the organization (Kumar et al., 2008; August et al., 2006).

Expectancy Theory

Expectancy theory has been used in numerous studies involving motivation in the workplace (Van Eerde et al., 1996). Expectancy theory has strong empirical support (Burton et al., 1992), is straightforward and easily understood by both practitioners and researchers (Fudge et al., 1999), and is applicable to practice (Sanchez et al., 2000). Further, expectancy theory enables a multidimensional diagnostic approach to motivation

(Sanchez et al., 2000; Ilgen et al., 1981; Courtney et al., 1983; DeSanctis, 1983). Expectancy theory explains motivation as a result of a multi-level assessment (Galbraith et al., 1967) including "perceptions of the environment and expectations based on these perceptions" (Brouer et al., 2011, p. 870). Expectancy theory shares the higher-order vs. lower-order outcome orientation espoused by many behavioral theorists (e.g. Carver et al., 1982; Wiener, 1948). *First-order outcomes* are the behaviors resulting from effort, while *second-order outcomes* are the ultimate outcomes resulting from the behavior (Sanchez et al., 2000). Specifically, expectancy theory—also referred to as VIE theory—offers a set of three motivational antecedents consisting of (1) valence, (2) instrumentality, and (3) expectancy (Ellingson et al., 2011).

Valence

Valence is the preference of one outcome over another (or all others) (Vroom, 1964). Valence is not the true satisfaction of an outcome, but rather the anticipated satisfaction (Vroom, 1964). This is an important distinction as valence serves as a motivator toward future action in expectancy theory. Actual satisfaction contributes to valence formulation only to the extent that past satisfaction influences future preferences (Ellingson et al., 2011). Valence can also be described as an assessment of the attractiveness of success (Feather, 1969).

In expectancy theory, valence is oriented toward higher-order outcomes (Sanchez et al., 2000; Ellingson et al., 2011). For the purposes of this study, *security valence* is defined as an insider's affinity for the protection of his or her firm from information security risks. The outcome referent of security valence (i.e., the security of the firm) distinguishes it from behavioral attitudes (Taylor et al., 1995; Anderson et al., 2010;

Ajzen, 1991). Security valence is associated with the attractiveness of protecting the firm (e.g. valence of the higher-order goal) and not the attitude toward the protective behavior itself (e.g. attitude about PMBs).Therefore, according to expectancy theory, it is the security-related outcome and not the attractiveness of the protective behavior itself which motivates performance of PMBs. In addition to valence perceptions, behavioral motivation is also reliant upon assessments of instrumentality and expectancy.

Instrumentality and Expectancy

Concomitant with valence, expectancy theory posits a dual-level model of motivation consisting of instrumentality and expectancy. Like valence, instrumentality is oriented toward higher-order outcomes. *Instrumentality* is an individual's perception that successfully enacting a behavior will lead to an ultimate (i.e. second-order) outcome (Vroom, 1964). Vroom (1964) describes instrumentality an "outcome-outcome association." Conversely, *expectancy* is an "action-outcome association" and is defined as a perception that an individual's efforts will lead to the intended behavior (Vroom, 1964). Therefore, expectancy theory provides a distinction between first- and second-order probabilities: (1) a first-order probability (e.g. expectancy) is the likelihood that given appropriate effort, an action can be taken, and (2) a second-order probability (e.g. instrumentality) is the likelihood that successfully taking an action will lead to a desired ultimate outcome.

The distinction between instrumentality and expectancy is important and has received considerable treatment in the behavioral literature. Bandura (1977) describes the distinction.

> People can give up trying because they lack a sense of efficacy in achieving the required behavior, or they may be assured of their capabilities but give up trying because they expect their behavior to have no effect on an unresponsive environment or to be consistently punished. These two separable expectancy sources of futility have quite different antecedents and remedial implications. To alter efficacy-based futility requires development of competencies and expectations of personal effectiveness. By contrast, to change outcome-based futility necessitates changes in prevailing environmental contingencies that restore the instrumental value of the competencies that people already possess (pp. 204-205).

Expectancy theory explains that expectancy and instrumentality have unique antecedents and consequences. The diagnostic nature of expectancy theory (Sanchez et al., 2000; Ilgen et al., 1981) makes it an attractive approach for establishing the antecedents of PMBs. In this study, I define *security instrumentality* as the perception that securing one's work-related information will protect the organization from security threats, and *security expectancy* as the perception that with ample effort one can protect his or her work-related information. Security instrumentality and expectancy, combined with valence, influence insiders' motivation to and withdrawal from the performance of PMBs.

Motivation and Withdrawal

Expectancy theory is often examined in terms of positive motivation (i.e. motivation toward an outcome) (Sanchez et al., 2000; DeSanctis, 1983; Fudge et al., 1999). However, facets of expectancy theory can be linked to positive, negative, or neutral perceptions (Vroom, 1964). Lack of instrumentality, for example, is linked to perceptions of helplessness (Dweck, 1975), wherein the helpless individual has no expectation of behavioral contingency (Diener et al., 1980; Abramson et al., 1978). In

other words, individuals who perceive themselves to be helpless expect that their actions—no matter how well performed—will not lead to the desired ultimate outcome (Diener et al., 1980; Maier et al., 1976).

Perceptions of expectancy provide task-related (i.e. first-order) motivation (Ellingson et al., 2011). Individuals lacking expectancy may see themselves as unskilled (Brouer et al., 2011), while those lacking instrumentality feel helpless due to some insurmountable personal or environmental circumstances (Diener et al., 1980; Maier et al., 1976). Therefore, expectancy is associated with motivation to attempt the task motivated at the task-level (Vroom, 1964; Brouer et al., 2011). Individuals lacking instrumentality, however, often feel helpless and psychologically distance themselves from the uncontrollable situation through a process of psychological withdrawal (Dweck, 1975).

Psychological withdrawal is the psychological equivalent of physical withdrawal, which can be either organizational-level psychological withdrawal or simply the withdrawal "from participation in a prescribed role" (Hulin et al., 1985, p. 233). Withdrawal can be the result of a preference (Hom et al., 2012), a mechanism for avoiding stress (Keaveney et al., 1993), or the result of unfavorable expectancies (Carver et al., 1982). For the purpose of this research, *security withdrawal* is defined as the psychological withdrawal from participation in security roles (e.g. PMBs). The role of security withdrawal has received considerably less attention in the security literature than other antecedents to security behaviors. The general schema of learned helplessness and expectancy theory is depicted in Figure 2.1.

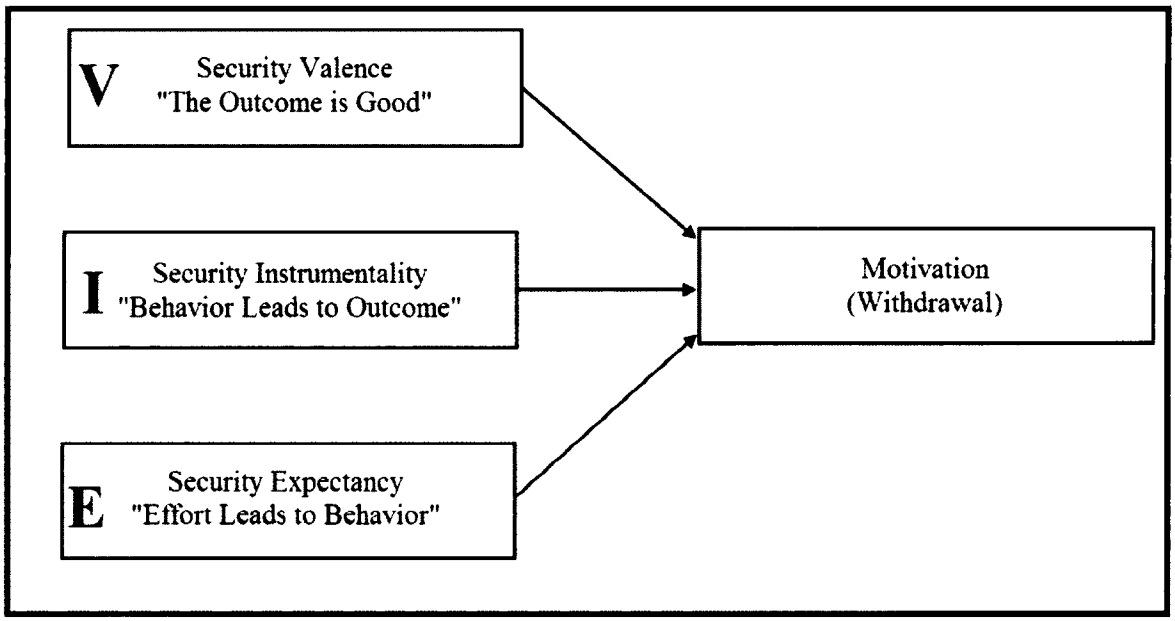


Figure 2.1 *Expectancy Theory Schema – VIE Model of Security Motivation/Withdrawal*

Security, Education, Training, and Awareness

Each component of the VIE model of security motivation/withdrawal provides unique insight into insiders' behavior. To the extent that valence, instrumentality, and expectancies can be influenced by organizations, behavioral outcomes are likewise influenced. As it relates to security, SETA programs are the mechanism by which organizations inform users of security threats, establish the responsibilities of the employees, and detail the consequences of failing to comply (D'Arcy et al., 2009; Straub et al., 1998). It follows that SETA programs should relate directly to the expectancy measures. In this way, expectancy theory provides a diagnostic framework for the positive impact of SETA programs.

Prior research has largely described the role of SETA programs in deterring inappropriate behaviors within an organization (Lee et al., 2002). Serving this purpose, organizations often employ SETA programs to provide individuals with a prescribed response to a given security threat (Zafar et al., 2009; Siponen et al., 2010), as well as to

persuade the user that a failure to comply is amply detrimental so as to deter security lapses (Straub et al., 1998). Recently the relationship between SETA and deterrence has been supported empirically (D'Arcy et al., 2009). However, a well-developed program should not only provide training related to security policy compliance, but should also maintain a program of keeping users aware of evolving security threats (Whitman, 2003). Further, to the extent that SETA programs influence the expectancy dimensions (i.e., valence, instrumentality, expectancy), SETA may be shown to be an effective tool in motivating insiders to protect their organizations' information and information systems by the performance of PMBs. The role of SETA on the expectancy dimensions is examined in this research to evaluate the potential motivational efficacy of SETA programs.

Psychological Capital

In addition to the direct impact of expectancy dimensions on motivation and withdrawal, expectancy theory is also related to malleable personal characteristics (Luthans et al., 2010) which have been shown to be an important consideration for security-related behavior (e.g. Myyry et al., 2009; Workman et al., 2008; Leach, 2003) . One such conceptualization of personal characteristics, PsyCap, has emerged out of the positive psychology movement (Luthans et al., 2007a). *Positive psychology* is "the study of the conditions and processes that contribute to the flourishing or optimal functioning of people, groups, and institutions" (Gable et al., 2005), and PsyCap is a construct of positive "psychological resource capabilities" which are open to development (Luthans et

al., 2009). PsyCap is a higher-order construct composed of distinct yet related core tenets of positive psychology of hope, resilience, optimism, and self-efficacy (Luthans et al., 2007b).

As a component of positive psychology, PsyCap is uniquely applicable to the present study because positive psychology has the optimal functioning of the average person as its subject (Seligman et al., 2000; Sheldon et al., 2001). PsyCap has also received broad acceptance in business research and beyond (Avey et al., 2009; Walumbwa et al., 2011; Avey et al., 2010; Peterson et al., 2011). PsyCap has been linked to a number of positive personal and organizational outcomes such as job performance and satisfaction (Luthans et al., 2007a), low absenteeism (Avey et al., 2006), low turnover and stress (Avey et al., 2009), as well as increased citizenship and decreased deviance (Avey et al., 2011). Finally, PsyCap has been shown to mediate important relationships between perceptions of organizational and behavioral environment and actual behavior (Luthans et al., 2008).

PsyCap Hope can be defined as a "positive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287; Luthans et al., 2007a). *PsyCap Resilience* "is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans et al., 2007a, p. 546; Masten, 2001; Masten et al., 2002). Resilience can also be thought of simply as "the positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702; Luthans et al., 2007a). *PsyCap Optimism* is defined as that characteristic that is held by individuals who

"expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985). *PsyCap Self-Efficacy* is role-breadth self-efficacy and is defined as "the employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66; Luthans et al., 2007a).

PsyCap can be viewed through a resource lens (Luthans et al., 2007b; Hobfoll, 1989; Hobfoll, 2002). Hobfoll (1989) stipulates that individuals require resources to function and will seek to gain available resources and when possible conserve unnecessarily expended resources. Thus, the conservation of resources entails two components: the building up of resources and the conservation of resources. PsyCap as a resource can be built at the facet level by micro-intervention or at the construct level by macro-intervention such as a supportive climate (Luthans et al., 2008). Resources are either "centrally valued in their own right" or "as a means to obtain centrally valued ends" (Hobfoll, 2002). PsyCap can also be viewed as adaptive in that not only does PsyCap embody a positive psychological state, as a psychological construct it serves meaningful ends. For instance, PsyCap has been shown to provide a necessary psychological resource for psychological well-being (Culbertson et al., 2010).

Lastly, a distinguishing quality of PsyCap–and perhaps one reason that it has been so widely considered—is that it has been shown to be composed of characteristics that are state-like rather than trait-like. This distinction between state- and trait-like characteristics is important as it differentiates those characteristics which are innate and inflexible from those which are malleable and developable (Zuckerman, 1983; Fugate et

al., 2012). Trainable characteristics are especially critical in a security context as they can be developed within an organization to enhance organizational security. PsyCap has been shown to be developable (Luthans et al., 2007a; Luthans et al., 2006a; Peterson et al., 2011); therefore, any benefits to firm security which can be shown to be attributable to PsyCap can be influenced by an organization through an investment in employees' PsyCap. This ductile quality of PsyCap distinguishes it from other, more stable, traits like "The Big Five" personality traits (Goldberg, 1990) and the higher order "Core Self-Evaluation" (Judge et al., 2001; Luthans et al., 2007a). Peterson (2012) notes:

> "People's locus of control and self-esteem are things a manager probably can't change significantly within a few weeks. Psychological capital is more malleable. We're not born hopeful, resilient, optimistic, efficacious people. We learn these things."

The facets of PsyCap and established facet-level development strategies are summarized in Table 2.1.

Table 2.1

Summary of PsyCap Characteristics

PsyCap Component	Definition	Micro-Development
PsyCap Self-Efficacy	"[T]he employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66)	• Mastery experiences • Modeling and vicarious learning • Social persuasion • Physiological and psychological arousal
PsyCap Hope	"[P]ositive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287).	• Goal-setting • Participation • Contingency planning for alternative pathways to attain goals
PsyCap Optimism	Characterizes individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985).	• Leniency for the past • Appreciation for the present • Opportunity-seeking for the future
PsyCap Resilience	"[T]he positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702)	• Asset-focused strategies such as enhancing employability • Risk-focused strategies such as proactive avoidance of adversity • Process-focused strategies to influence the interpretation of adverse events
Adapted from descriptions in *Psychological capital: Developing the human competitive edge,* Luthans, Youssef, et al. (2007b).		

Protection-Motivated Behaviors

PMBs are the volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS in which that information is stored, collected, disseminated, and/or manipulated from information-security threats (Posey et al., 2013). PMBs are in-role and extra-role behaviors that an insider may undertake which protect the firm's information and information systems (Posey et al., 2013). Posey et al.(2013) categorized PMBs into a systematic-based taxonomy made up of fourteen categories (see Table 2.2) for summary, and Posey et al. (2013) for full discussion).

Table 2.2

PMB Roles

Identified Cluster Number and Name
4. Appropriate data entry and management
3. Policy-driven awareness and action
8. Wireless installation
2. Protection against unauthorized exposure
7. Verbal and electronic sensitive-information protection
9. Widely applicable security etiquette
12. Account protection
11. Co-worker reliance
13. Immediate reporting of suspicious behavior
1. Legitimate e-mail handling
6. Secure software, e-mail, and Internet use
5. Document conversion
10. Distinctive security etiquette
14. Equipment location and storage
Table 2.2 from Posey, Roberts, Lowry, Bennett, & Courtney, 2013

As a general class of behaviors, PMBs are robust to the varying security policies that are inevitably found across organizations. For example, compliance with an explicit security policy is clearly an in-role behavior, but the specific behaviors required for that compliance vary across firms (Bulgurcu et al., 2010).

Research Model and Hypotheses

SETA programs are often employed in order to inform employees about the various threats to the organization's security as well as to train employees to recognize threats and enact various security roles (D'Arcy et al., 2009; Straub et al., 1998; Lee et al., 2002). Education, training, and awareness each relate to the motivational dimensions espoused in expectancy theory. SETA is expected to increase an insider's perception of behavioral expectancy, outcome instrumentality, and outcome valence. That is, SETA is expected to (1) enhance the perception that insider's efforts will lead to successful

performance of the desired security behavior (security expectancy), (2) increase an insider's perception that the behavior will lead ultimately to the security of the firm (security instrumentality), and (3) influence insiders' perceptions that protecting the firm is good (security valence).

H1: SETA will be positively related to users' security valence.

H2: SETA will be positively related to users' security instrumentality.

H3: SETA will be positively related to users' security expectancy.

Security expectancies are first-order perceptions (Vroom, 1964; Galbraith et al., 1967) and are hypothesized to be positively related to motivation to protect the firm, deemed protection motivation. As explained in expectancy theory, the perception that effort will lead to performance of a behavior is directly linked to behavioral motivation. On the other hand, instrumentality (or lack thereof) is a second-order perception and relates to ultimate outcomes. Security instrumentality is an insider's perception that their protective behaviors will ultimately protect the firm. A lack of instrumentality is linked to helplessness and withdrawal from behavioral attempts (Dweck, 1975; Carver et al., 1982). Therefore, perceptions of expectancy and instrumentality each have a unique impact on PMBs through increased protection motivation and decreased security withdrawal.

Expectancy theory further explains that favorability of an outcome or valence provides a motivational stimulus as well. Therefore, positive security valence (i.e. favorable perception of protecting the firm from security threats) is expected to be positively related to protection motivation. Conversely, security valence is expected to be negatively related to security withdrawal. Vroom (1964, p. 15) notes, "[a] positive (or

approach) motive signifies that outcomes which are members of the class have positive valence, and a negative (or avoidance) motive signifies that outcomes in the class have negative valence."

H4: Security expectancy will be positively related to users' protection motivation.

H5: Security instrumentality will be negatively related to security withdrawal.

H6: Security valence will be positively related to users' protection motivation.

H7: Security valence will be negatively related to security withdrawal.

PsyCap is composed of psychological resource capabilities (Luthans et al., 2007b; Luthans et al., 2009) and is directly related to individual's perceptions of expectancy and instrumentality. Security expectancy and instrumentality are hypothesized to be positively related to each of the PsyCap characteristics in related, yet distinct ways. First, expectancy is expected to have a positive impact on PsyCap self-efficacy, which is role-breadth self-efficacy (Parker, 1998; Luthans et al., 2007b), by virtue of the increased confidence of an insider that he or she can successfully enact instrumental security behaviors. In a similar way, PsyCap hope and PsyCap optimism are expected to be increased by expectancies and instrumentalities, as those with perceptions of expectancy and instrumentality will feel able to enact pathways instrumental to reaching goals (PsyCap hope) and will be more likely to believe that positive security outcomes can be achieved (PsyCap optimism). Finally, employees' perceived expectancy and instrumentality are hypothesized to be related to PsyCap resilience, as individuals who see themselves as able to enact instrumental security behaviors will be more equipped to adapt in the face of security challenges and bounce back after failed attempts to enact PMBs.

H8: Security expectancy will be positively related to users' PsyCap.

H9: Security instrumentality will be positively related to users' PsyCap.

Whether viewing PsyCap as a psychological resource or simply a positive psychological state, the previously established links between PsyCap and organizational outcomes provide a basis for the relationship between PsyCap and protection motivation. For example, PsyCap has been positively linked to an increase in both job performance and satisfaction (Luthans et al., 2007a) as well as increased organizational commitment and citizenship (Avey et al., 2011). As security continues to be adapted into organizational strategy through security policy and otherwise, an increase in job performance, which includes security policy compliance, will lead to an increase in organizational security (Siponen et al., 2006; Herath et al., 2009; Bulgurcu et al., 2010). The positive impact of job satisfaction, commitment, and citizenship are closely linked and are supported by findings that individuals who are satisfied with their jobs are better organizational citizens and can be expected to perform both in-role and extra-role behaviors to support the organization (Bateman et al., 1983; Williams et al., 1991). The performance of protective behaviors is the focus of this research and as such, it is expected that PsyCap will increase protection motivation in part by virtue of the established relationships with increased job performance, satisfaction, commitment, and citizenship.

H10: PsyCap will be positively related to protection motivation.

PsyCap, has also been shown to reduce unfavorable outcomes such as absenteeism (Avey et al., 2006), turnover and stress (Avey et al., 2009), and cynicism and deviance (Avey et al., 2011). Therefore, PsyCap's reduction of withdrawal-related

outcomes is hypothesized to reduce the security-vulnerability created by security omission through the reduction of security withdrawal.

H11: PsyCap will be negatively related to security withdrawal.

In line with the theories of planned behavior (TPB) and reasoned action (TRA) (Ajzen, 1991; Ajzen et al., 1972) which contend that intentions often mediate important relationships with behavior, protection motivation is conceptualized as the intention to protect the organization. Therefore, protection motivation is hypothesized to lead to PMBs. Finally, security withdrawal is the withdrawal from security roles, and is hypothesized to lead to an omission of PMBs (see Figure 2.2).

H12: Protection Motivation will be positively related to PMBs.

H13: Security withdrawal will be negatively related to PMBs.

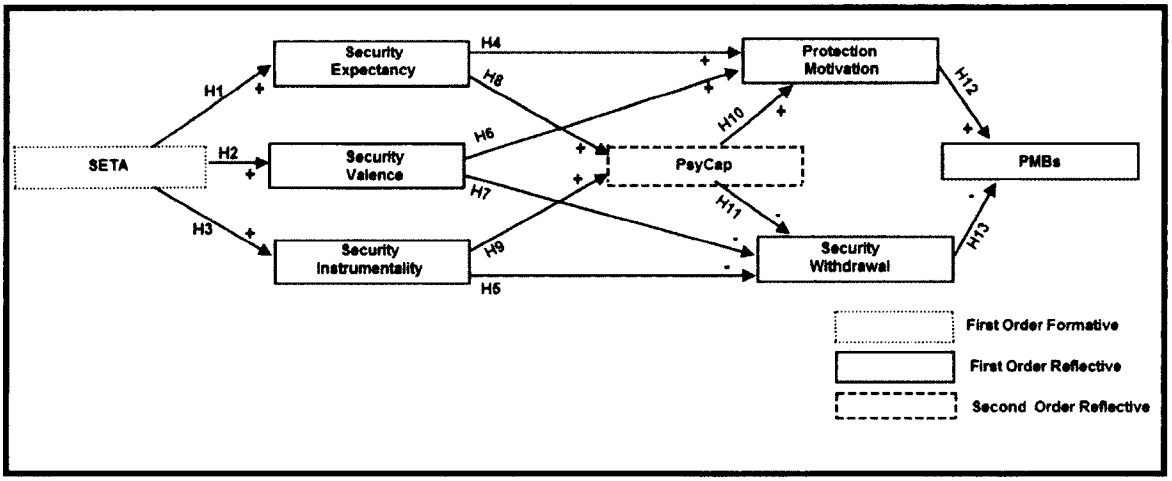


Figure 2.2 *Research Model*

Measurement Models

As shown in Figure 2.2, the research model utilizes three distinct latent model structures: first-order reflective constructs, a first-order formative construct, and a second-order reflective construct. Construct specification is a topic of considerable

interest in IS research, as the field seeks to employ second generation techniques with both theoretical and statistical validity (Bagozzi, 2011; Gefen et al., 2000; Gefen et al., 2011; Straub et al., 2004; Jarvis et al., 2003). The ultimate goal of all model specification is to appropriately model theoretical relationships; therefore, the on-going discussion regarding the theoretical justification and statistical validity is an important one (Aguirre-Urreta et al., 2012; Jarvis et al., 2012).

The various forms of model specification are "derived from the fact that (a) a first-order construct can have either formative or reflective indicators, and (b) those first-order constructs can, themselves, be either formative or reflective indicators of an underlying second-order construct" (Jarvis et al., 2003). Constructs defined as first- and second-order reflective appear most often in business research (Jarvis et al., 2003), and specify that the indicators at each level "reflect" the latent variable (Straub et al., 2004; Jarvis et al., 2012). All of the constructs in this study were adapted from prior research and retained the specification of the published measures.

Research Methodology

The multi-dimensional research model was tested empirically using survey research methodology. The instrumentation for the survey was developed based on a thorough literature review. Where possible, the items were adapted from prior research. All the items included in the final survey were subjected to subject matter expert review and were pilot tested before executing the final survey.

Study Measures

SETA was measured using five items in this study. *SETA* measures an individual's perception that the organization provides training to educate employees about

information security issues and security responsibilities. As in previous research, SETA was measured with a formative construct consisting of five items (D'Arcy et al., 2009).

Security valence, instrumentality, and expectancy (VIE) measures were adapted from existing scales of the expectancy dimensions (Sanchez et al., 2000). The original items measured VIE in a test-taking situation. In order to adapt the measures into a security context, the measures were altered to capture the perception of security-related valence, instrumentality, and expectancy. The items adapted to measure security valence, ascertain the extent to which the respondent perceives keeping the organization safe from security threats is attractive or good. The items for security instrumentality were adapted to reflect the perception that security their work-related information would secure the organization from information security threats. Finally, security expectancy items were adapted to measure the perception that with adequate effort the respondent could secure his or her information at work. An example of an item used to measure security valence is "It would be good to protect my organization from security threats." An example of an item used to measure security instrumentality is "If I protect my information and computer at work, my organization has a good chance of being protected from security threats." An example of an item used to measure security expectancy is "I can protect my information and computer at work if I put some effort into it."

PsyCap was measured using the questionnaire developed by Luthans, Youssef et al. (2007b). The PsyCap Questionnaire includes twenty-four items (six for each of the four characteristics). The PsyCap items were all developed from prior literature and have consistently exhibited validity and test/retest reliability throughout the business literature. (Luthans et al., 2007a; Luthans et al., 2007b).

PsyCap hope measures state-hope and is "responsive to events in the lives of people" (Snyder et al., 1996, p. 321). PsyCap hope captures both the agency and pathway components of hope, and an example of an item measuring PsyCap Hope is "I can think of many ways to reach my current work goals"(Luthans et al., 2007b). *PsyCap Resilience* measures an individual's ability to bounce back or to take stressful things at work in stride (Wagnild et al., 1993). An example of an item measuring resilience is "I usually take stressful things at work in stride" (Luthans et al., 2007b). *PsyCap optimism* measures an individual's state-belief that "good rather than bad things will happen to them" (Scheier et al., 1985, p. 219). An example of an item measuring PsyCap optimism is "I approach this job as if 'every cloud has a silver lining'"(Luthans et al., 2007b). Lastly, *PsyCap self-efficacy* measures the state-like role-breadth self-efficacy and is based on Parker's (1998) self-efficacy scale. An example of an item measuring *PsyCap self-efficacy* is "I feel confident analyzing a long-term problem to find a solution" (Luthans et al., 2007b).

Protection motivation was measured as an intention to perform protective behaviors. The scale was developed in accordance with the view of Ajzen and Fishbein (1972) that intention mediates important antecedents of behavior. As such, protection motivation is modeled as a behavioral intention in the way of the theory of planned behavior (Ajzen, 1991). Posey (2010) developed a four item scale which was used to assess an individual's protection motivation. A sample item measuring protection motivation is "I intend to protect my organization from its information security threats."

Security withdrawal is a state of psychological withdrawal in which individuals' experience withdrawal-like symptoms such as denying, ignoring, or refusing to respond

to security threats (Keaveney et al., 1993). The items used to measure security withdrawal were adapted to reflect a psychological withdrawal from security from established measures of psychological distancing (Beaudry et al., 2010). *Psychological distancing* is "the effort one expends to direct one's attention away from the situation and detach oneself from it" (Beaudry et al., 2010, p. 699). In order to assess security withdrawal, insiders were asked to indicate the extent to which they engaged in psychological distancing when dealing with a security threat. An example of an item measuring security withdrawal is "When confronted with a security threat... I told myself that there was nothing I could do about the threat to my organization's information security."

PMBs were measured with a five-item scale developed based on a taxonomy of protection-motivated behaviors (Posey et al., 2013). The taxonomy identifies fourteen categories of behaviors and reflective items measuring a general class of PMBs were developed using a MIMIC model (see Posey, in press for full explanation of item development). An item assessing the performance of PMBs is "I tried to safeguard my organization's information and information systems from their information security threats."

Analysis and Results

The research model was analyzed in a two-step procedure as recommended by methodologists (Gerbing et al., 1988). The analysis utilized covariance-based structural equation modeling (SEM) platform Mplus (Muthén et al., 1998-2010). In the first step, a confirmatory factor analysis (CFA) was run in Mplus in order to establish the validity of the measures to be included in the subsequent structural model. Upon confirmation of the

validity of the research model, the hypothesized research model was assessed using SEM in Mplus. Prior to the collection of the data for the final analysis, the instrument was pilot tested to confirm the validity of the measures.

Pilot Study

Critical to any study is the validity and reliability of the measures employed (Straub, 1989; Gefen et al., 2011). As recommended, whenever possible the scales included in this study were employed as previously published (Straub et al., 2004). The instrument was pilot tested with a sample of 42 MBA students from a large public university in the Southeastern United States. All the students used for the pilot were either currently employed or had previous work experience. The descriptive statistics of the pilot sample are summarized in Table 2.3.

Table 2.3

Descriptive Statistics of Pilot Sample

Average Age		24.26
Average Organizational Tenure		1.66
Gender	Female	31%
	Male	69%
IT Position		4.8%
Management		12.2%

The data from the pilot test was used to examine the validity of the reflective measures to be used in the study. The pilot test construct statistics were ascertained using partial least squares structural equation modeling (PLS-SEM) in SmartPLS (Ringle et al., 2005). Overall, the results of the pilot test provide evidence of the initial validity of the

measures to be used in the full study. The construct loadings from the pilot test are summarized in Table 2.4.

Table 2.4

Pilot Study Construct Loadings

	Security Expectancy	Security Instrumentality	Security Valence	Security Withdrawal	Protection Motivation	PMBs	PsyCap
SE1	0.932						
SE2	0.934						
SE3	0.865						
SI1		0.931					
SI2		0.856					
SI3		0.904					
SI4		0.922					
SV1			0.936				
SV2			0.931				
SV3			0.975				
SW1				0.634			
SW2				0.915			
SW3				0.875			
PM1					0.931		
PM2					0.915		
PM3					0.916		
PM4					0.892		
PMB1						0.949	
PMB2						0.926	
PMB3						0.946	
PMB4						0.874	
PMB5						0.941	
PCO							0.808
PCSE							0.896
PCH							0.914
PCR							0.925

In addition to viewing the standardized loadings, I also examined the convergent and divergent validity of the constructs by calculating the latent variable correlations, the

Cronbach's alpha, and the average variance extracted (AVE) for each of the constructs. The convergent and divergent statistics are summarized in Table 2.5.

Table 2.5

Pilot Study Construct Correlations

	Security Expectancy (SE)	Security Instrumentality (SI)	Security Valence (SV)	Security Withdrawal (SW)	Protection Motivation (PM)	PMB	PsyCap	Cronbach's α
SE	**0.83***							0.8971
SI	0.6017	**0.82**						0.9247
SV	0.3122	0.4366	**0.90**					0.9429
SW	-0.4662	-0.6665	-0.4345	**0.67**				0.7557
PM	0.7789	0.6611	0.5314	-0.6334	**0.83**			0.9337
PMB	0.4279	0.4837	0.6104	-0.4493	0.6104	**0.86**		0.9593
Psy Cap	0.4578	0.434	0.4595	-0.1913	0.4595	0.3871	**0.79**	0.9189
***AVE's** bolded along diagonal								

Primary Study

After analyzing the results of the pilot test and confirming the initial validity of the instrumentation, responses were collected from a sample of 414 organizational insiders. On-line panels are especially appropriate for gathering security data as they offer full anonymity, not simply confidentiality. Given the sensitive nature of security responses, anonymity is required to encourage candid responses, and panels provide increased anonymity in multiple ways. First, the researchers never know the identity of the respondents, and the privacy of respondents is guaranteed and governed by the data provider. Second, respondents' real and perceived anonymity is enhanced by having access to the survey outside of their organization's network and computers. Providing anonymous, off-site access to self-report surveys has been shown to be adequate and appropriate for the elicitation of self-reported incidences of sensitive and even socially

undesirable behaviors such as protection-motivated behaviors (Posey et al., 2013) and organizational deviance (Bennett et al., 2000; Bennett et al., 2003). The descriptive statistics of the primary sample are summarized in Table 2.6.

Table 2.6

Descriptive Statistics of Primary Sample

Average Age		45.59
Average Organizational Tenure		10.58
Gender	Female	53.1%
	Male	46.9%
Education	Some high school	0.2%
	High school diploma	11.4%
	Some college	25.6%
	Undergraduate degree	41.5%
	Master's degree	16.4%
	Doctorate/Professional degree	4.8%
IT Position		15.2%
Management		33.8%

Construct Validity

For the reflective measures included in the structural model, the standardized factor loadings from a CFA analysis were considered along with the Cronbach's alphas. Also, the convergent and discriminant validity of measures in the structural model were assessed with average variance extracted (AVE) and the Fornell-Larker criterion (comparison of squared correlations with AVEs) as recommended (Hair et al., 2006; Hair et al., 2014). This study also employed one construct which was specified as formative in prior research, SETA (D'Arcy et al., 2009). The validity of formative measures is assessed differently than that of reflective measures (Hair et al., 2014). In order to assess the validity of SETA, first, the content validly was examined for the present study.

Second, the collinearity of the formative items was assessed by calculating the indicator correlation matrix and the variance inflation factor (VIF) of each indicator. Finally, the statistical and practical significance of each formative indicator was assessed through the significance and magnitude of the coefficient (see Table 2.7).

Table 2.7

Full Measures in Study & Validity Statistics

CFA of Reflective Items: Chi-Squared = 1758.36 d.f. = 794; CFI: 0.94; RMSEA: 0.054						
Items	Measures	Scale[i]	Spec.[ii]	Mean	STD	Load.
Security Valence (SV)	Adapted from Sanchez et al. (2000) Instructions: "Please indicate your level of agreement with the following statements about information-security threats to your organization."	Scale	Spec.	Mean	STD	Load.
SV-1	I would like to protect my organization from information security threats.	a	R	5.89	1.230	0.970
SV-2	It would be good to protect my organization from information security threats.	a	R	6.02	1.191	0.894
SV-3	I want to protect my organization from information security threats.	a	R	5.94	1.202	0.945
Security Expectancy (SE)	Adapted from Sanchez et al. (2000) Instructions: "Please indicate your level of agreement with the following statements about information-security threats to your organization."	Scale	Spec.	Mean	STD	Load.
SE-1	If I try my best to perform security tasks, I can successfully protect my work-related information.	a	R	5.44	1.225	0.908
SE-2	If I concentrate and try hard then I can secure my work-related information.	a	R	5.32	1.208	0.887
SE-3	I can protect my work-related information if I put some effort into it.	a	R	5.49	1.210	0.911
Security Instru-mentality (SI)	Adapted from Sanchez et al. (2000) Instructions: "Please indicate your level of agreement with the following statements about information-security threats to your organization."	Scale	Spec.	Mean	STD	Load.
SI-1	If I protect my work-related information, my organization has a good chance of being protected from security threats.	a	R	5.30	1.361	0.941

Table 2.7 (Continued)

SI-2	I think my organization will be protected from security threats if I can secure my work-related information.	a	R	5.24	1.389	0.912
SI-3	How well I protect my work-related information will affect whether my organization is protected from security threats.	a	R	5.24	1.509	0.911
SI-4	The better I am at securing my work-related information, the more likely my organization will be protected from security threats.	a	R	5.18	1.355	0.897
Security Withdrawal (SW)	Adapted from Beaudry et al. (2010) Instructions: "Indicate how often you reacted in the following ways when confronted with a threat to your organization's information security."	Scale	Spec.	Mean	STD	Load.
	"Indicate how often you reacted in the following ways when confronted with a threat to your organization's information security."	b	R			
SW-1	I told myself that time would take care of the threat to my organization's information security.	b	R	2.95	1.673	0.715
SW-2	I told myself that there was nothing I could do about the threat to my organization's information security.	b	R	3.08	1.638	0.856
SW-3	I tried not to worry about the threat to my organization's information security.	b	R	3.87	1.637	0.652
Protection Motivation (PM)	Posey (2010) Instructions: "Please indicate your level of agreement with the following statements about information-security threats to your organization."	Scale	Spec.	Mean	STD	Load.
PM-1	I intend to protect my organization from its information security threats.	a	R	5.48	1.314	0.931
PM-2	My intentions to prevent my organization's information security threats from being successful are high.	a	R	5.36	1.355	0.892
PM-3	It is likely that I will engage in activities that protect my organization's information and information systems from security threats.	a	R	5.28	1.424	0.863
PM-4	I intend to expend effort to protect my organization from its information security threats.	a	R	5.23	1.369	0.864
PsyCap Hope (PCH)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Spec.	Mean	STD	Load.
PCH-1	If I should find myself in a jam at work, I could think of many ways to get out of it.	a	R	5.34	1.057	0.721

Table 2.7 (Continued)

PCH-2	At the present time, I am energetically pursuing my work goals.	a	R	5.14	1.334	0.675
PCH-4	Right now I see myself as being pretty successful at work.	a	R	5.41	1.054	0.764
PCH-5	I can think of many ways to reach my current work goals.	a	R	5.29	1.246	0.794
PCH-6	At this time, I am meeting the work goals that I set for myself.	a	R	5.45	1.118	0.763
PsyCap Resilience (PCR)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Spec.	Mean	STD	Load.
PCR-2	I usually manage difficulties one way or another at work.	a	R	5.64	.989	0.814
PCR-3	I can be "on my own," so to speak, at work if I have to.	a	R	6.01	1.069	0.714
PCR-4	I usually take stressful things at work in stride.	a	R	5.18	1.202	0.668
PCR-5	I can get through difficult times at work because I've experienced difficulty before.	a	R	5.61	1.069	0.850
PCR-6	I feel I can handle many things at a time at this job.	a	R	5.65	1.111	0.786
PsyCap Optimism (PCO)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Spec.	Mean	STD	Load.
PCO-1	When things are uncertain for me at work, I usually expect the best.	a	R	4.81	1.263	0.773
PCO-3	I always look on the bright side of things regarding my job.	a	R	5.03	1.521	0.845
PCO-4	I'm optimistic about what will happen to me in the future as it pertains to work.	a	R	5.09	1.277	0.765
PCO-6	I approach this job as if "every cloud has a silver lining."	a	R	4.96	1.421	0.762
PsyCap Self-Efficacy (PCSE)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Spec.	Mean	STD	Load.
PCSE-1	I feel confident analyzing a long-term problem to find a solution.	a	R	5.43	1.143	0.786
PCSE-2	I feel confident in representing my work area in meetings with management.	a	R	5.45	1.274	0.782
PCSE-3	I feel confident contributing to discussions about the company's strategy.	a	R	5.05	1.375	0.752
PCSE-4	I feel confident helping to set targets/goals in my work area.	a	R	5.543	1.250	0.742
PCSE-5	I feel confident contacting people outside the company (e.g., suppliers, customers) to discuss problems.	a	R	5.17	1.482	0.625

Table 2.7 (Continued)

PCSE-6	I feel confident presenting information to a group of colleagues.	a	R	5.32	1.347	0.755
Protection Motivated Behaviors (PMB)	(Posey, 2010) Instructions: "Given the following statements, on what basis did you engage in the stated behaviors in the last year?"	Scale	Spec.	Mean	STD	Load.
PMB-1	I actively attempted to protect my organization's information and computerized information systems	b	R	4.87	1.900	0.944
PMB-2	I tried to safeguard my organization's information and information systems from their information security threats	b	R	4.94	1.877	0.906
PMB-3	I took committed action to prevent information security threats to my firm's information and computer systems from being successful	b	R	4.52	1.983	0.863
PMB-4	I purposefully defended my organization from information security threats to its information and computerized information systems	b	R	4.36	1.994	0.813
PMB-5	I earnestly attempted to keep my organization's information and computer systems from harm produced by information security threats	b	R	4.90	1.886	0.924
Security Education Training Awareness (SETA)	D'Arcy et al. (2009) Instructions: "Please indicate your level of agreement with the following statements about your organization."	Scale	Spec.	Mean	STD	Load.
SETA-1	My organization provides training to help employees improve their awareness of computer and information security issues.	a	F	4.51	1.846	0.081
SETA-3	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	a	F	4.50	1.870	0.112
SETA-4	My organization educates employees on their computer security responsibilities.	a	F	4.82	1.795	0.529
SETA-5	In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	a	F	4.59	1.854	0.349

(R) = reverse scored item
[i]Scale: a) Strongly Disagree – Strongly Agree; b) Never – Always
[ii]Specification: R) reflective F) formative

As shown in Table 2.7, most of the standardized loadings of the reflective items were above a conservative 0.70 cutoff criterion. A loading of 0.70 indicates that the

associated latent variable accounts for 50% of the variance in the indicator (Hair et al., 2006; Hair et al., 2014). The Cronbach's alpha of each construct was within the recommendations of prior research (Nunnally, 1978) (see Table 2.8). Finally, the constructs exhibit convergence and discriminance as indicated by the ratio of Fornell-Larker statistic and latent variable correlations of ≤ 1.

Table 2.8

Primary Study Reflective Construct Correlations

	Security Expectancy (SE)	Security Instrumentality (SI)	Security Valence (SV)	Security Withdrawal (SW)	Protection Motivation (PM)	PMB	PsyCap	Cronbach's α
SE	**0.81***							0.93
SI	0.78	**0.84**						0.95
SV	0.69	0.64	**0.88**					0.96
SW	-0.19	-0.17	-0.25	**0.56**				0.78
PM	0.79	0.79	0.75	-0.18	**0.79**			0.94
PMB	0.59	0.66	0.56	-0.04	0.75	**0.79**		0.96
PsyCap	0.63	0.53	0.56	-0.15	0.46	0.39	**0.71**	0.95
*AVE's bolded along diagonal								

The validity of SETA was assessed according to the recommendations for formatively specified constructs (Hair et al., 2014). First, the content validity of the SETA measure was established. Formative measures are modeled to include no measure error (Bagozzi, 2011); therefore, the formative items are said to fully explain the latent variable. An error in content validity is manifest in the absence of an item which should be included in order to fully represent the construct domain. The formative item measuring SETA was taken directly from prior research (D'Arcy et al., 2009). In its prior use, SETA was validated in a similar context (security) and to a similar population

(organizational insiders). Based on the previous establishment of SETA and an assessment of the items forming SETA, the construct was determined to be content valid. Second, the collinearity of the items was assessed by assessing the correlations among items and running regressions of each item on the others in order to ascertain the VIF level of each item. Items with a VIF of greater than ten are said to suffer from multicollinearity, while those with a VIF of five or less are conservatively assessed to have no multicollinearity (D'Arcy et al., 2009; Hair et al., 2014; Hair et al., 2006). The range of VIFs was 3.0 to 4.3 with the average for each SETA item reported in Table 2.9.

Table 2.9

SETA Item Correlations & VIFs

	SETA 1	SETA 3	SETA 4	SETA 5
SETA 1	**3.7**			
SETA 3	.786***	**3.4**		
SETA 4	.794***	.761***	**3.7**	
SETA 5	.793***	.839***	.801***	**3.2**
*** p=0.001; **avg. VIF**. bolded along diagonal				

Structural Model

Finally, the hypothesized relationships in the research model were tested using SEM. The Chi-Squared statistic and degrees of freedom (X^2=2552.8 and d.f.=967; X^2 to d.f. ratio = 2.6) along with a goodness of fit index (CFI =0.90) and a badness of fit index (RMSEA=.06) all indicate that the final structural model has good fit overall (Hu et al., 1999; Kline, 2010). Moreover, nine of thirteen hypothesized relationships were significant and in the predicted direction. (see Table 2.10)

Table 2.10

Structural Model Results

Chi-Squared = 2552.8; d.f.= 967 CFI=0.91; RMSEA=0.06				
Hyp.	Hypothesis (direction)	Path Coefficient	p-value	Significance (two-tailed)
H1	**SETA→ Security expectancy (+)**	**0.520**	**<0.001**	***
H2	**SETA→ Security valence (+)**	**0.403**	**<0.001**	***
H3	**SETA→ Security instrumentality (+)**	**0.514**	**<0.001**	***
H4	**Security expectancy → Protection motivation (+)**	**0.572**	**<0.001**	***
H5	Security instrumentality → Security withdrawal (-)	-0.002	0.983	n/s
H6	**Security valence → Protection motivation (+)**	**0.453**	**<0.001**	***
H7	**Security valence → Security withdrawal (-)**	**-0.242**	**0.001**	***
H8	**Security expectancy → PsyCap (+)**	**0.572**	**<0.001**	***
H9	**Security instrumentality → PsyCap (+)**	**0.139**	**0.044**	*
H10	PsyCap → Protection motivation (+)	0.020	0.668	n/s
H11	PsyCap → Security withdrawal (-)	-0.015	0.827	n/s
H12	**Protection motivation → PMBs (+)**	**0.734**	**<0.001**	***
H13	**Security withdrawal → PMBs (-)**	**0.11**	**0.009**	**
Bold = supported; *p=0.05; **p=0.01; ***p=0.001; n/s=not significant				

Controls and Rival Explanations

To substantiate the findings of the structural model, the analysis was performed again including several controls. As can be seen in Table 2.11, controls for age, tenure, gender, and whether the individual had a managerial or an IT position had no significant impact on the performance of PMBs. Additionally, potential rival explanations of PMBs were tested in order to isolate the impact of the expectancy model. Security locus of control, managerial support for security, and social desirability were all included as potential rival explanations of the performance of PMBs. Again, as can be seen in Table 2.11, none of the controls were statistically related to the performance of PMBs. Further, the expectancy model was fully robust to the inclusion of the controls and the substantive

variables in the study suffered no appreciable loss of impact or significance when tested in concert with a plethora of controls. The research model is shown in Figure 2.3.

Table 2.11

Structural Model Results Including Controls

Chi-Squared = 4104.921; d.f.= 1660 CFI=0.87; RMSEA=0.06				
Hyp.	Hypothesis (direction)	Path Coefficient	p-value	Significance (two-tailed)
H1	**SETA→ Security expectancy (+)**	**0.520**	**<0.001**	***
H2	**SETA→ Security valence (+)**	**0.403**	**<0.001**	***
H3	**SETA→ Security instrumentality (+)**	**0.514**	**<0.001**	***
H4	**Security expectancy → Protection motivation (+)**	**0.573**	**<0.001**	***
H5	Security instrumentality → Security withdrawal (-)	-0.003	0.964	n/s
H6	**Security valence → Protection motivation (+)**	**0.454**	**<0.001**	***
H7	**Security valence → Security withdrawal (-)**	**-0.240**	**0.001**	***
H8	**Security expectancy → PsyCap (+)**	**0.553**	**<0.001**	***
H9	**Security instrumentality → PsyCap (+)**	**0.139**	**0.045**	*
H10	PsyCap → Protection motivation (+)	0.017	0.718	n/s
H11	PsyCap → Security withdrawal (-)	-0.016	0.816	n/s
H12	**Protection motivation → PMBs (+)**	**0.722**	**<0.001**	***
H13	**Security withdrawal → PMBs (-)**	**0.097**	**0.031**	*
Controls				
	Age	0.004	0.457	n/s
	Tenure	-0.005	0.513	n/s
	Manager	0.227	0.101	n/s
	IT Position	0.147	0.422	n/s
	Gender	-0.061	0.635	n/s
	Security Locus of Control	0.046	0.425	n/s
	Managerial Support for Security	-0.083	0.141	n/s
	Social Desirability	0.071	0.196	n/s
Bold = supported; *p=0.05; **p=0.01; ***p=0.001; n/s=not significant				

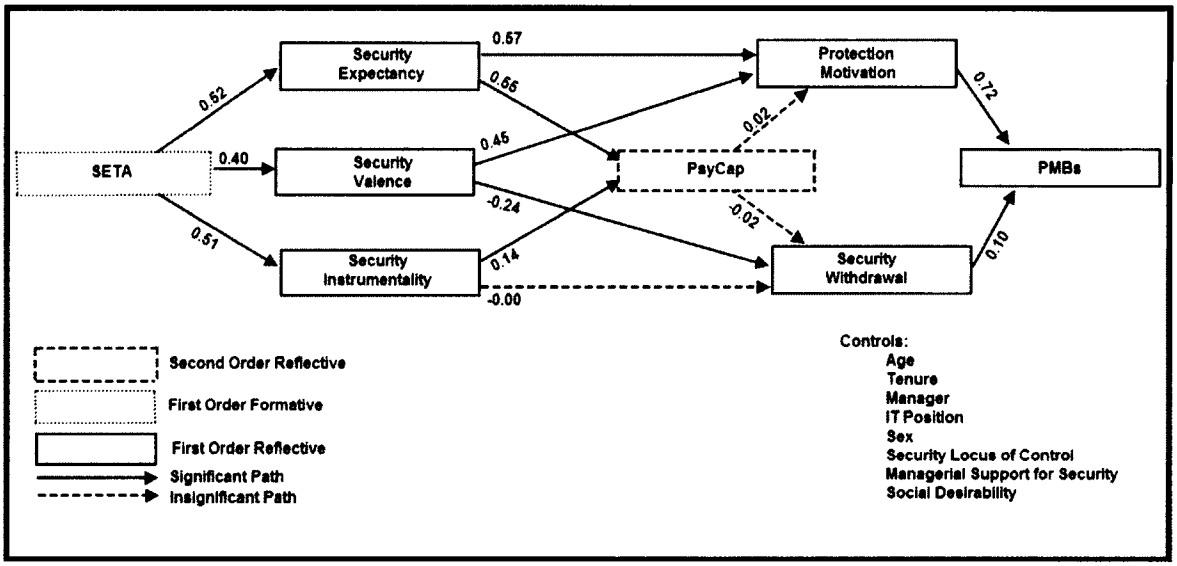


Figure 2.3 *Research Model*

Discussion

The expectancy-based security model provides a robust, multidimensional framework of PMB motivation. The role of insiders as protectors of the firm's security is an evolving role that is based on the realization that insiders are uniquely able to protect their firm's information and information systems (Posey et al., 2013). The results of this study elucidate the impact of expectancy dimensions on the motivation to and withdrawal from performance of security behaviors. As predicted, security expectancy is positively related to the motivation to protect the firm's information and IS. Additionally, security valence is positively related to protection motivation and negatively related to security withdrawal.

In addition to finding support for relationships espoused in Vroom's (1964) expectancy theory, I also found support for the role of SETA in influencing insiders' security-related valence, instrumentality, and expectancies. The positive impact of training was shown through the relationship between SETA and all three expectancy

measures. Second, as hypothesized, expectancy and instrumentality build insiders' psychological resource capabilities manifested in their positive relationship with PsyCap. Finally, as predicted protection motivation is positively related to PMBs. Therefore, the intention to protect the firm from security threats significantly impacts whether or not an insider proactively attempts to protect their firm's information and information system.

The direct role of PsyCap on security motivation was not supported in the research model. PsyCap was not significantly related to either motivation or withdrawal. However, the findings support a relationship between security and PsyCap. Specifically, the expectancy theory measures were shown to increase the PsyCap of individuals. One potential explanation of the insignificant relationship between PsyCap and protection motivation is the substantial explanatory power of the security expectancy measures, which leave little variance in protection motivation for PsyCap to explain.

I found one significant relationship which was in the opposite direction of the hypothesis, the relationship between security withdrawal and PMBs. This finding is seemingly counter-intuitive at first given the concept of security withdrawal. However, security withdrawal as measured in self-report requires that the individual actively identify potential security threats and then cope with the threat by psychologically distancing him or herself from the performance of security behaviors. This identification of security threats may be confounding the impact of security withdrawal by implicitly including an identification of potential security threats. The significant negative relationship between security valence and withdrawal supports this assertion by indicating that individuals who believe it is good to protect their firm from security threats are less likely to withdraw psychologically from security behaviors. In this way,

the nuance of psychological withdrawal is made evident as psychological withdrawal does not necessarily negatively relate to intention to protect the firm. Ergo, an individual may not be convinced that protecting the firm is good, and may withdraw psychologically from security behaviors yet refrain from malicious intent or maintain an—albeit weaker—intention to protect the firm.

Implications and Contributions

This research makes several important contributions to the behavioral information security literature. First, the expectancy theory-based research model establishes evidence of SETA's positive relationship with insiders' expectancies. The positive relationship between SETA and each of the expectancy dimensions provides an important framework for the influence of SETA on insiders' motivation to and withdrawal from protective behaviors. The diagnostic nature of expectancy theory makes it uniquely suited for establishing training roles, and the significance of SETA on expectancy, instrumentality, and valance support a multi-dimensional framework for SETA development. Organizations seeking to increase security can effectively develop insiders' behavioral expectancies, outcome instrumentalities, and outcome valences via SETA programs.

Complementary to the recently established deterring effect of SETA (D'Arcy et al., 2009), this research also provides support for a broad and positive impact of SETA programs. In addition to the direct relationship between SETA and expectancy measures, the findings establish an indirect relationship between SETA and PsyCap. Therefore, organizations which employ SETA programs to impact the valence, instrumentality and

expectancies of insiders will have the compounding organizational impact of insiders' increased PsyCap which has been found to be related to myriad positive organizational outcomes (see Table 2.12).

Table 2.12

Summary of Key Findings

Key finding	**Significance to research**	**Significance to practice**
SETA's influence on the three expectancy dimensions	Provides a diagnostic framework for future research on SETA effectiveness.	Provides support for SETA as an effective mechanism for developing the expectancy facets of insiders.
Expectancy dimensions influence on insiders' PsyCap	Provides evidence of the broadly positive impact of SETA through the development of expectancy dimensions.	Links security to positive psychological resources, and provides a framework of PsyCap development for organizations through SETA programs.
Expectancy dimensions influence on motivation to/withdrawal from security behaviors	Provides behavioral information security research with a framework within which to investigate insiders' motivation to and withdrawal from security behaviors.	Provides a framework for SETA in which training for the expectancy dimensions increases insiders' motivation to protect the firm.
Expectancy Theory model robust to controls for (1) demographics (2) managerial support, (3) social desirability, and (4) locus of control	Isolates the results of the research model to the expectancy dimensions which are shown to be malleable through SETA.	Provides support for the robustness of organizational security programs which incorporate manipulation of expectancy dimensions.

The multi-dimensional expectancy-based approach to security is also an effective model of PMBs, accounting for 53% of the variance in PMBs. Further, security valence and security expectancy together explained 66% of the variance in insider's protection motivation. This indicates that organizations that are able to successfully affect insiders'

security expectancy and valence can make a substantial impact in influencing the protection motivation of their employees. These relationships are important for the development of future organizational initiatives and SETA programs. The impact of SETA was significant and similar on all three measures in the VIE model, indicating that to a large extent SETA programs equally influence each facet of expectancy.

Limitations and Future Research

There are inherent limitations in self-reported security research, and to a large extent this research is no exception. However, due to the absence of observational data of actual security behaviors, survey instruments are an accepted medium for ascertaining the behavior of insiders. I took recommended precautions to ensure that individual anonymity was preserved and responses were uninhibited. Additionally, the data analyzed in this research was collected at a cross-sectional level with differences measured between randomly surveyed organizational insiders. Expectancy theory has been employed at both the within and between individual levels in past research. While some have argued that expectancy theory is most appropriate for analyzing motivational changes within individuals, the robust performance of expectancy between individuals supports its use as a framework of security behavior across individuals. Given the significance of the research model, future research can use this expectancy-based framework to examine within individual impacts resulting from manipulations such as training sessions.

In the research model, SETA significantly explained 26%, 27%, and 16% of the variance in instrumentality, expectancy, and valence, respectively. This underscores the remaining antecedents to expectancy measures to be uncovered by future research. A

significant relationship between the expectancy theory measures of instrumentality and expectancy and PsyCap was established in this research. However, PsyCap was not significantly related to either protection motivation or to security withdrawal. Future research should continue to examine the relationship between insiders' PsyCap and security behaviors. Specifically, the role of PsyCap as a resource for security behavior, as a potential moderator of important relationships, and as a dependent variable in IS research should be explored.

Conclusion

This chapter developed and applied an expectancy theory based research model of protective security behaviors. The results of the study indicate that expectancy theory is an appropriate framework within which to view the performance of PMBs. Nine of the thirteen hypothesized relationships were significant and in the hypothesized direction. Security expectancies build insiders' PsyCap and also provide motivation to protect the firm. Security valence buffers insider's from withdrawing from security behaviors and simultaneously motivates toward protection of the firm. Security instrumentality also works to build insiders' PsyCap. The positive impact of SETA was also made clear in the results of the structural model, being significantly related to the three facets of the expectancy model (VIE). The indirect effect of SETA on PsyCap is an important finding and underscores the broadly positive impact of security training. Finally, the results were robust to a number of important controls, both demographic related, personality related, and security related.

CHAPTER 3

THE ADAPTIVE ROLE OF EMOTION IN INFORMATION SECURITY: BROADENING THE THEORETICAL REPERTOIRE

Introduction

Humans are broadly influenced by experiences of emotion. An individual's emotional reaction is often an adaptational intermediary between stimuli and corresponding behavior (Lazarus, 1991). In information systems (IS), emotive-behavioral models have provided a complementary view of adaptation to the plethora of cognitive-behavioral models (e.g. Venkatesh et al., 2003; Davis, 1989). Behavioral models are of increasing interest in IS security as practitioners and researchers recognize that the information security of organizations is at the mercy of organizational insiders (Moore et al., 2008; Boss et al., 2009; D'Arcy et al., 2007). *Organizational insiders* include not only technology specialists, but all employees and organizational agents with access to the information system and informational resources in the fulfillment of organizational responsibilities (Posey et al., 2013; Shaw et al., 1998). In today's environment of enterprise-wide systems and ubiquitous computing, these insiders have the greatest access to their organization's information and IS (Stanton et al., 2006a). For example, over 50% of firms worldwide now allow employees to use mobile devices for tasks such

as sales force automation, project management, and email (Symantec, 2012). Another 89% of firms have enabled employees to access organizationally relevant material from employee-owned devices, a phenomenon dubbed "bring your own device" (BYOD) (Bradley et al., 2012).

Given the influence of insiders' behavior on security and the central role of emotion in adaptation, the study of emotion in IS security is warranted. Further, all organizations are emotionally-laden (Amabile et al., 2005). Emotion in the workplace, however, is not merely an artifact of the organization itself, but rather a manifestation of the multitudes of *person-environment relationships* which constitute the larger organization (Lazarus, 1991). Lazarus (1991 loc. 570) notes, "the basic unit of this person-environment relationship is an adaptational encounter." IS security is rife with such adaptational encounters as insiders are assailed with increasingly sophisticated threats to their firms' security (Hamill et al., 2005). IS security has no framework for the consideration of the broad spectrum of emotions, but rather—as in the broader organizational literature (Fredrickson, 1998)—has often considered only the role of negative emotions, particularly fear (e.g. Johnston et al., 2010). However, emotional stimuli often elicit multiple emotions of varying intensities simultaneously (Lazarus et al., 1984; Lazarus, 1991; Beaudry et al., 2010). The broaden-and-build theory (Fredrickson, 1998; Fredrickson, 2001) provides a multi-dimensional framework of emotions which includes the often neglected positive emotions. The *broaden-and-build theory* posits that positive emotions "broaden the scope of attention and thought-action repertoires," (Fredrickson et al., 2005) while simultaneously building lasting psychological resources (Fredrickson, 1998; Fredrickson, 2001; Fredrickson et al., 2005).

An individual's *thought-action repertoire* is the collection of the thoughts and behaviors, which are cognitively available to the actor (Fredrickson et al., 2005).

The broaden and build theory is an outworking of a new positive direction in the larger field of psychology known as the positive psychology movement (Seligman et al., 2000). *Positive psychology* is "the study of the conditions and processes that contribute to the flourishing or optimal functioning of people, groups, and institutions" (Gable et al., 2005). Positive psychological resources such as those described in the broaden-and-build theory have received increased attention in positive psychology. One such conceptualization of positive psychological resources is psychological capital (PsyCap). *PsyCap* is a construct of positive "psychological resource capabilities" which are open to development (Luthans et al., 2009). PsyCap is a higher order construct composed of distinct yet related core tenets of positive psychology of hope, resilience, optimism, and self-efficacy (Luthans et al., 2007b).

PsyCap is uniquely applicable in behavioral information security research because the optimal functioning of the "average person" is its subject (Sheldon et al., 2001). Similarly, IS security research has taken an interest in the role of ordinary insiders, including their ability to increase their firms' information security (Posey et al., 2013; Albrechtsen et al., 2009; Stanton et al., 2005). Recently, a taxonomy of protection-motivated behaviors (PMBs) has explicated the ways in which these ordinary insiders can protect their organizations' information and IS (Posey et al., 2013). *PMBs* are the volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS in which that

information is stored, collected, disseminated, and/or manipulated from information-security threats (Posey et al., 2013).

Whether through security policy compliance (Herath et al., 2009) or PMBs (Posey et al., 2013), insiders seeking to practice safe computing are faced with an increasingly complex environment within which to protect the organization's IS. Organizations often play on the emotions of employees to elicit security behaviors by employing appeals to emotion, such as fear (Johnston et al., 2010; Anderson et al., 2010; Herath et al., 2009; Lee et al., 2009). However, as the role of emotion continues to become increasingly important in IS, a thorough treatment of the role of emotion requires the spectrum of emotions be considered (Beaudry et al., 2010). The broaden-and-build theory provides a model for considering the role of emotions, both positive and negative in adaptation. The goal of this paper is to integrate a framework of emotions (Beaudry et al., 2010) with the broaden-and-build theory (Fredrickson, 1998, 2001) to thoroughly examine the adaptive role of emotions in information security.

Emotion and Adaptation in IS

> *It is inconceivable to me that there could be an approach to the mind, or to human and animal adaptation, in which the emotions are not a key component. Failure to give emotion a central role puts theoretical and research psychology out of step with human preoccupations from the beginning of recorded time* (Lazarus, 1991 loc. 125-127).

IS research continues to adapt to the evolving role of technology in the workplace and society at large. Along this pursuit, Abraham et al. (2013) describe the need to add adaptive mechanisms to the "theoretical repertoire" of IS research. A principle tenet of adaptation is the belief that the most suited creatures survive (i.e. "survival of the fittest").The organizational and economic implications of survival of the fittest are

widespread from firm survival (Gimeno et al., 1997) to the adoption of technology (Hantula et al., 2011; Kock, 2009). From an evolutionary perspective, emotions play the adaptive role of fit enhancement (Nesse et al., 2009). Hence, when fit is challenged, negative emotions are positively adaptive and vice versa. It has been the role of emotions to elicit some innate or adaptive response which generally has increased the survival of our species (Nesse et al., 2009). Therefore, emotions can be viewed as either an innate coping mechanism or an evolved remnant of historically (and presently) adaptive responses.

Behavioral research has begun to acknowledge the role of adaptation in the explanation of behavioral responses (Capra et al., 2011; Griskevicius et al., 2011; Hantula et al., 2011). However, a general framework for describing phenomena in light of adaptive responses has not yet been created (Saad, 2011). The *broaden-and-build theory* of positive emotions offers an integrated framework of emotions. Application of the broaden-and-build theory provides explanation of the complex relationship between emotional stimuli and adaptation. Additionally, the broaden-and-build theory elucidates the role of emotions (both positive and negative) on cognition, behavior, and the psychological resources of the emotional being.

Affect and Emotion in IS Security

Since William James (1884) first asked *What is an emotion?*, and even long before, philosophers, psychologists, and other behaviorists have grappled with the meaning and implications of emotions (Solomon, 2008). Even now there remain inconsistencies in the conception of emotions in contrast to other affective states, such as sensory pleasure and positive mood (Fredrickson et al., 2008). For many (including the

author), an acceptable differentiator is that emotions, both negative and positive, have a specific referent (Beaudry et al., 2010; Lazarus, 1991; Smith et al., 1990). This is in the vein of what Frijda (1988) called "situational meaning." Therefore, affect can be viewed as an "umbrella for a set of more specific mental processes including emotions, moods, and (possibly) attitudes," and emotion a referent specific "mental state of readiness" (Bagozzi et al., 1999, p. 184).

Positive affect is often concomitant with positive emotion though more stable and relatively long lasting (Fredrickson, 2001; Forgas et al., 2001). Further, as opposed to the specificity of emotions, positive affect is often considered a measure of general happiness (Culbertson et al., 2010). Both positive emotions and affect, however, facilitate motivation or approach behavior (Carver et al., 1990; Cacioppo et al., 1999). The stable nature of general affect over time has caused it to become conceptualized as a trait-like characteristic of individuals (Kaplan et al., 2009). Persistent or trait-like affect is associated with categories of workplace behavior (Bennett et al., 2003). For example, positive affect has been linked to organizational citizenship behaviors (OCBs), while a negative affect has been linked to a decrease in OCBs along with an increase in counterproductive work behaviors (CWBs) (Kaplan et al., 2009).

Beaudry and Pinsonneault (2010) developed a framework for classifying specific emotions in IS based on the work of Lazarus and his colleagues (Lazarus et al., 1984; Folkman et al., 1986). Lazarus and Folkman (1984, p. 26) describe a coping process for individuals confronted with "any event in which the person feels his or her adaptive resources to be taxed or exceeded." According to Lazarus, taxing stimuli initiate a two stage appraisal process: (1) a primary appraisal and (2) a secondary appraisal (Lazarus et

al., 1984). During the primary appraisal, an individual assesses the stimulus as either irrelevant, benign-positive, or stressful, while the secondary appraisal is a judgment of control. Stressful appraisals are further delineated as harm/loss, threat, or challenge (Lazarus et al., 1984). These primary, secondary, and stress appraisals can be seen in the emotional framework presented by Beaudry and Pinsonneault (2010) (see Figure 3.1).

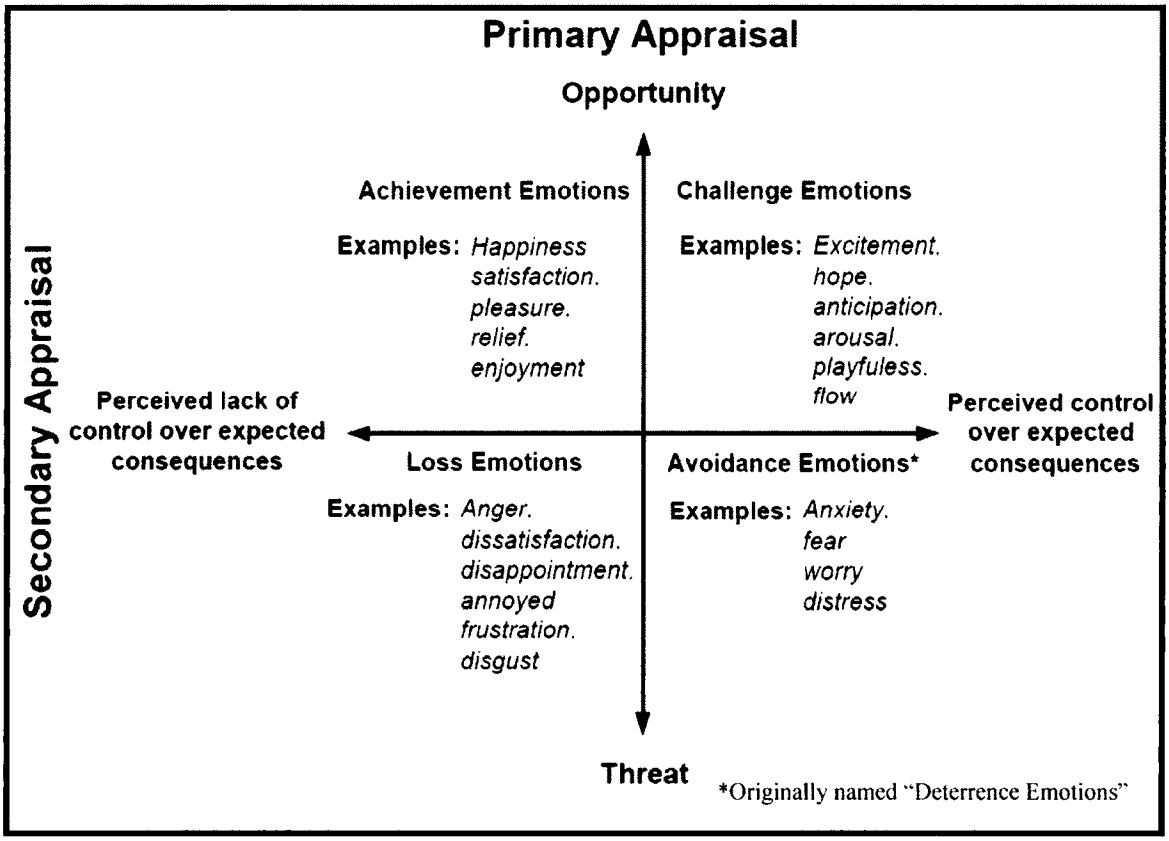


Figure 3.1 *Classification of Emotions – Adapted from Beaudry & Pinsonneault (2010)*

Beaudry and Pinsonneault's (2010) framework of emotions is instrumental in the depiction of discrete emotions as experiences of emotions are often overlapping and varying in intensity (Lazarus et al., 1984). The framework can also be viewed as categorizing emotions as either positive (above the x-axis) or negative (below the x-axis). The distinction of positive and negative emotions is warranted as positive and negative

emotions have been found to be relatively independent and impact behavior and cognition differently (Bagozzi et al., 1999; Cenfetelli, 2004; Fredrickson, 2001). When stimuli are appraised as fit enhancing (i.e. an opportunity), the emotions elicited have a positive valence, whereas stimuli assessed as challenging fit (i.e. a threat) elicit negative emotions (Nesse et al., 2009; Beaudry et al., 2010). In this way, Beaudry and Pinsonneault's (2010) emotional framework illustrates the similarities between appraisal theories of emotion and adaptive approaches to emotion (Nesse et al., 2009).

The impact of negative emotions has received greater consideration in the behavioral literature than positive emotions (Fredrickson, 1998). IS security has more often considered the role of negative emotions as well, most frequently through fear appeals (Johnston et al., 2010; Anderson et al., 2010; Herath et al., 2009; Lee et al., 2009). Compared to the information technology (IT) usage literature (Beaudry et al., 2010; Venkatesh, 1999; Davis et al., 1992; Cenfetelli, 2004), the role of positive emotions has been examined less often in IS security. Additionally, when emotion has been considered it has been in the form of fear which is a single discrete negative emotion (Egloff et al., 2003; DeSteno et al., 2004; Nabi, 2002). *Discrete emotions* "each reflect a unique person-environment relationship, and thus are associated with different goals and action tendencies designed to achieve those goals" (Nabi, 2002, p. 205). The role of emotion across the spectrum of positive and negative discrete emotions is examined in this chapter through the integration of Beaudry and Pinsonneault's (2010) framework of emotion with Fredrickson's (2001, 1998) broaden-and-build theory.

The Broaden-and-Build Theory

The broaden-and-build theory posits that positive emotions broaden an individual's thought-action repertoire and increase the ability to process large amounts of information through a broadened scope of attention (Fredrickson, 2001). Positive emotions also build lasting psychological resources over time (Fredrickson, 1998; Fredrickson, 2001; Fredrickson et al., 2005). Therefore, implicit in the broaden-and-build theory are three distinct roles of emotions: (1) a broadening role, (2) a narrowing role, and (3) a building role (Fredrickson et al., 2005).

Broadening Role

The broadening role of positive emotions impacts individuals in two distinct ways. First, positive emotions broaden an individual's ability to recognize and process external cues (e.g. broadens scope of attention and ability to process large amounts of information). Second, positive emotions broaden an individual's thought-action repertoire. A broadened scope of attention and cognitive processing is in line with Isen's (1999) assertions that positive affect generally influences "memory, learning, problem solving and creativity, and flexibility in thinking." A broadened scope of attention also increases cognitive variation, and cognitive variation results in an increase in the number of original ideas generated (Amabile et al., 2005). In the same way, as individuals broaden their processing of conditions relative to an issue, creativity in problem solving arises (Fredrickson, 2004; Amabile et al., 2005). As employees seek to protect the firm through their use of and interactions with the firm's IS (Posey et al., 2013), the increased cognitive agility and broadened information processing that result from positive emotions

(Isen, 1999; Fredrickson, 2004; Fredrickson et al., 2005; Amabile et al., 2005) provide insiders with important resources for contributing to IS security.

Positive emotions also lead to the broadening of an individual's thought-action repertoire. An individual's thought-action repertoire is the collection of thoughts and actions cognitively available to an individual at a moment in time (Fredrickson et al., 2005). Therefore, enactment of the PMBs identified by Posey et al (2013) is contingent upon the availability of these behaviors to the actor at the time of the behavioral stimulus. The broaden-and-build theory implies insiders experiencing positive emotions are more likely to have the known behaviors cognitively accessible in the face of a security threat. In this way, the broaden-and-build theory offers a partial remedy for the "knowing-doing" gap of security behaviors (Workman et al., 2008) by explaining that security-related thought and behavioral diversity is enhanced by positive emotions.

Narrowing Role

In contrast to the broadening role of positive emotions, there is an implicit narrowing role of negative emotions in the broaden-and-build theory (Fredrickson et al., 2005). That there is a narrowing role to complement the broadening role does not imply an inverse relationship between positive and negative emotions, however. Positive and negative emotions do not produce opposite behaviors, but rather work in different ways on cognition and behavior altogether (Isen, 1999). The narrowing role of emotions is rooted heavily in the aforementioned adaptive role of emotions. Negative emotions elicit *specific action tendencies* based on adaptive needs (Fredrickson et al., 2005; Cosmides et al., 2000). These adaptive tendencies are considered to be innate and often evolved mechanisms for increasing fit and therefore survival (Öhman et al., 2001; Cosmides et

al., 2000; Nesse et al., 2009). For example, when fit is threatened, negative emotions such as fear may be stimulated, which produce a state of readiness for a specific action such as "flight" (Nesse et al., 2009; Bagozzi et al., 1999). In this way, as predicted by the broaden-and-build theory, the specific tendency brought about by fear narrows the thought-action repertoire of the individual experiencing the negative emotion (Fredrickson, 1998; Fredrickson, 2001).

Beaudry and Pinsonneault's (2010) original framework of emotions classified negative emotions associated with controllable consequences (e.g. fear, anxiety, worry, distress) as "deterrence emotions." However, these emotions are often associated with an action tendency of avoidance (Lazarus, 1991). Therefore, I have reclassified the bottom right quadrant of the emotional framework as "avoidance emotions." This is an appropriate reclassification as avoidance emotions are those which arise when an individual appraises a stimulus as threatening fit, yet perceives control over the outcome (i.e. the consequences are avoidable) (Beaudry et al., 2010; Nesse et al., 2009). Avoidance is an active adaptation due to the implied perception of control over the outcome (Carver et al., 1982). As IS security research continues to search for the conditions of efficacious emotional appeals (Crossler et al., 2012), the broaden-and-build theory is a useful framework for considering the role of emotions in relation to security behaviors. As explained by the theory, negative emotions narrow individual's thought-action repertoire and elicit an innate reaction.

Building Role

Finally, the broaden-and-build theory predicts that positive emotions build significant, lasting psychological resources such as resilience, optimism, and creativity

over time (Fredrickson, 2001; Fredrickson, 1998). In this way, the broaden-and-build theory can be seen as providing a framework for positive emotions in positive psychology (Fredrickson, 2001). Positive psychology has been described as "the study of the conditions and processes that contribute to the flourishing or optimal functioning of people, groups, and institutions" (Gable et al., 2005). In their introduction of positive psychology, Seligman and Csikszentmihalyi (2000) describe positive psychology as focused on "the good life," outlining positive characteristics such as well-being, optimism, hope, and happiness, among others. Fredrickson et al. (2002) note that these experiences of positive emotions provide an "upward spiral" toward lasting psychological resources. Core psychological resources associated with positive psychology have recently become recognized as an individual's PsyCap (Luthans et al., 2007a).

Psychological Capital

The broaden-and-build theory postulates that positive emotions build positive resources such as resilience and optimism (Fredrickson, 1998; Fredrickson, 2001; Fredrickson et al., 2005). As a higher order construct made up of hope, self-efficacy, resilience, and optimism (Luthans et al., 2007a), PsyCap is a higher order construct composed of positive resource capabilities (Luthans et al., 2009). PsyCap has received broad acceptance in business research and beyond (Avey et al., 2009; Walumbwa et al., 2011; Avey et al., 2010; Peterson et al., 2011). In addition, PsyCap has been linked to a number of positive personal and organizational outcomes such as job performance and satisfaction (Luthans et al., 2007a), low absenteeism (Avey et al., 2006), and low turnover and stress (Avey et al., 2009). PsyCap is also associated with increased citizenship and decreased deviance (Avey et al., 2011).

PsyCap Hope can be defined as a "positive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287; Luthans et al., 2007a). *PsyCap Resilience* "is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans et al., 2007a, p. 546; Masten, 2001; Masten et al., 2002). Resilience can also be thought of simply as "the positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702; Luthans et al., 2007a). *PsyCap Optimism* is defined as that characteristic that is held by individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985). *PsyCap Self-Efficacy* is a role-breadth self-efficacy and is defined as "the employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66; Luthans et al., 2007a).

An important distinction of PsyCap and perhaps one reason that it has been so widely considered is that it has been shown to be composed of characteristics that are state-like rather than trait-like. Though research has often relied on context to inform the true distinction between state and trait (Allen et al., 1981), there is an important distinction to be made between trait-like and state-like characteristics (Zuckerman, 1983; Fugate et al., 2012). This distinction is especially critical in a security context because PsyCap, a construct composed of state-like characteristics, has been shown to be developable (Luthans et al., 2007a; Luthans et al., 2006a; Peterson et al., 2011). This

ductile quality of PsyCap distinguishes it from other, more stable, traits like "The Big Five" personality traits (Goldberg, 1990) and the higher order "Core Self-Evaluation" (Judge et al., 2001; Luthans et al., 2007a). Therefore, any benefits to firm security which can be shown to be attributable to PsyCap can be influenced by an organization through an investment in employees' PsyCap.

PsyCap as a Resource

PsyCap is also composed of positive resource capabilities. Hobfoll (1989; 2002) stipulates that individuals require resources for functioning, and they will seek to gain available resources and when possible conserve unnecessarily expending resources. Therefore, the conservation of resources has two components: building of resources and conservation of resources. PsyCap as a resource can be built by either micro-intervention (Luthans et al., 2007b) or by macro-intervention such as a supportive climate (Luthans et al., 2008). In reference to conservation, resources are either "centrally valued in their own right" or "as a means to obtain centrally valued ends" (Hobfoll, 2002). PsyCap can be viewed as adaptive in that not only does PsyCap embody a positive psychological state, as a psychological construct it serves meaningful ends. For instance, PsyCap has been shown to provide a necessary psychological resource for psychological well-being (Culbertson et al., 2010) (see Table 3.1).

Table 3.1

Summary of PsyCap Characteristics

PsyCap Component	Definition	Micro-Development
PsyCap Self-Efficacy	"[T]he employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66)	1. Mastery experiences 2. Modeling and vicarious learning 3. Social persuasion 4. Physiological and psychological arousal
PsyCap Hope	"[P]ositive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287).	1. Goal-setting 2. Participation 3. Contingency planning for alternative pathways to attain goals
PsyCap Optimism	Characterizes individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985).	1. Leniency for the past 2. Appreciation for the present 3. Opportunity-seeking for the future
PsyCap Resilience	"[T]he positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702)	1. Asset-focused strategies such as enhancing employability 2. Risk-focused strategies such as proactive avoidance of adversity 3. Process-focused strategies to influence the interpretation of adverse events
Adapted from descriptions in *Psychological capital: Developing the human competitive edge*, Luthans, Youssef, et al. (2007b).		

Protection-Motivated Behaviors

Posey et al. (2013) identified PMBs as in- and extra-role behaviors that an insider may undertake which protect the firm's information and information systems. *PMBs* are the volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS in which that information is stored, collected, disseminated, and/or manipulated from information-security threats (Posey et al., 2013). These protective behaviors were organized into a systematic-based taxonomy of fourteen categories (see Table 3.2 for summary, and Posey

et al. (2013) for full discussion). As a general class of behaviors, PMBs are robust to the varying security policies that are inevitably found across organizations. For example, compliance with an explicit security policy is clearly an in-role behavior, but the specific behaviors required for that compliance vary across firms (Bulgurcu et al., 2010).

Table 3.2

PMB Clusters[i]

Identified Cluster Number and Name
4. Appropriate data entry and management
3. Policy-driven awareness and action
8. Wireless installation
2. Protection against unauthorized exposure
7. Verbal and electronic sensitive-information protection
9. Widely applicable security etiquette
12. Account protection
11. Co-worker reliance
13. Immediate reporting of suspicious behavior
1. Legitimate e-mail handling
6. Secure software, e-mail, and Internet use
5. Document conversion
10. Distinctive security etiquette
14. Equipment location and storage

[i]Table 3.2 from Posey, Roberts, Lowry, Bennett, & Courtney, 2013

Research Model and Hypotheses

This study examines the role of emotion in IS security by empirically testing a model which incorporates Beaudry and Pinsonneault's (2010) emotional framework into Fredrickson's (2001, 1998) broaden-and-build theory. As described, the broaden-and-build theory entails three implicit hypotheses which are tested in this research: (1) a broadening hypothesis, (2) a narrowing hypothesis, and (3) a building hypothesis. In order to assess the hypotheses, emotions were identified from each quadrant of Beaudry and Pinsonneault's (2010) framework of emotions. These discrete emotions arise out of

adaptive encounters and each elicit a distinct cognitive, psychological, or physiological response (Lazarus, 1991; Lazarus et al., 1984). Though each emotion has a specific stimulus or referent, a single stimulus may elicit multiple discrete emotions of varying intensity simultaneously (Lazarus, 1991). In order to assess the adaptive role of discrete emotion in performance of PMBs, the emotional reaction to thinking about protecting the organization's information and information system from security threats was ascertained from organizational insiders.

Challenge emotions arise out of an appraisal process which classifies an adaptation-related stimulus as an opportunity over which the individual perceives him or herself to have control (Beaudry et al., 2010). As such, challenge emotions are positive emotions which exhibit an apparent fit enhancement opportunity (Nesse et al., 2009). Lazarus (1991) describes one who has appraised a stimulus as a challenge. "A challenge makes one feel good, and there is apt to be a considerable expansion of one's functioning, with relevant thoughts coming easily and with a subjective impression that one is approaching the zenith of one's powers" (1991, loc 373). This broadened thought pattern elicited by challenge emotions mirrors the broadening hypothesis of the broaden-and-build theory. Further, the perceived control over the stimulus of challenge emotions exacerbates the approach tendency generally associated with positive emotions (Carver et al., 1990; Cacioppo et al., 1999). As an example, the challenge emotion excitement has been linked with task adaptation (Beaudry et al., 2010). It is hypothesized that the elicitation of challenge emotions will be positively related to PMBs.

H1: Challenge Emotions will be positively related to PMBs.

Achievement emotions arise out of an appraisal of an opportunity for fit enhancement with no perceived control over the outcome (Beaudry et al., 2010; Nesse et al., 2009). The broaden-and-build theory hypothesizes that certain positive emotions work to build lasting psychological resources such as those conceptualized in PsyCap. Fredrickson (2001) notes the building role of positive emotions. "Joy can have the incidental effect of building an individual's physical, intellectual, and social skills. Importantly, these new resources are durable and can be drawn on later, long after the instigating experience of joy has subsided" (p. 305) . Based on the building role of positive emotions in the broaden-and-build theory, achievement emotions elicited by the thought of protecting the organization from security threats will be positively related to PsyCap.

H2: Achievement emotions will be positively related to PsyCap.

Loss emotions arise out of an appraisal of a stimulus as being an uncontrollable threat to fitness (Beaudry et al., 2010; Nesse et al., 2009). As Lazarus (1991, loc. 108) notes: "[l]oss undermines our appreciation of life and may lead to withdrawal and depression." In that way, loss taxes one's psychological resources. PsyCap can be viewed as positive resources which are taxed by loss emotions. Therefore loss emotions are hypothesized to be negatively related to PsyCap.

H3: Loss emotions are negatively related to PsyCap.

Avoidance emotions arise out of a threat appraisal paired with perceived control over the outcome (Beaudry et al., 2010; Nesse et al., 2009). Perceptions of control are instrumental in motivating behavior of all kinds (Carver et al., 1982). The elicitation of avoidance emotions have been widely found to be effective at inducing threat-avoidance

behaviors in IS security (Johnston et al., 2010). However, the referent of the emotion has most often been a security threat (Johnston et al., 2010; Anderson et al., 2010; Herath et al., 2009; Lee et al., 2009). Therefore, by shifting the referent of the emotion from the threat itself to the protective behavior, it is expected that avoidance emotions will be *negatively* related to PMBs.

H4: Avoidance emotions will be negatively related to PMBs.

Whether viewing PsyCap as a psychological resource or simply a psychological state, the previously established links between PsyCap and organizational outcomes provide a basis for the relationship between PsyCap and PMBs. For example, PsyCap has been positively linked to an increase in both job performance and satisfaction (Luthans et al., 2007a) as well as increased organizational commitment and citizenship (Avey et al., 2011). As security continues to be adapted into organizational strategy through security policy and otherwise, an increase in job performance, which includes security policy compliance, will lead to an increase in organizational security (Siponen et al., 2006; Herath et al., 2009; Bulgurcu et al., 2010). The positive impact of job satisfaction, commitment, and citizenship are closely linked and are supported by findings that individuals who are satisfied with their jobs are better organizational citizens and can be expected to perform both in-role and extra-role behaviors to support the organization (Bateman et al., 1983; Williams et al., 1991). The performance of protective behaviors is the focus of this research and as such, it is expected that incorporating PsyCap will increase PMBs in part by virtue of the established relationships with increased job performance, satisfaction, commitment, and citizenship.

H5: PsyCap will be positively related to PMBs.

The preceding hypotheses deal with situational or referent-specific discrete emotions and their consequences. However, much research indicates that individuals are simultaneously impacted by relatively more stable and lingering affective states or even traits (Fredrickson, 2001; Forgas et al., 2001; Kaplan et al., 2009) . These more persistent dispositions are largely independent of one another and are generally referred to as positive affect and negative affect (Diener et al., 1984; Cenfetelli, 2004). Positive affect is linked to OCBs, and negative affect is related to a decrease in OCBs and to an increase in CWBs (Kaplan et al., 2009). Given these findings it is hypothesized that positive affect will have a positive relationship with PMBs, while negative affect will be negatively related to PMBs (see Figure 3.2).

H6: Positive Affect will be positively related to PMBs.

H7: Negative Affect will be negatively related to PMBs.

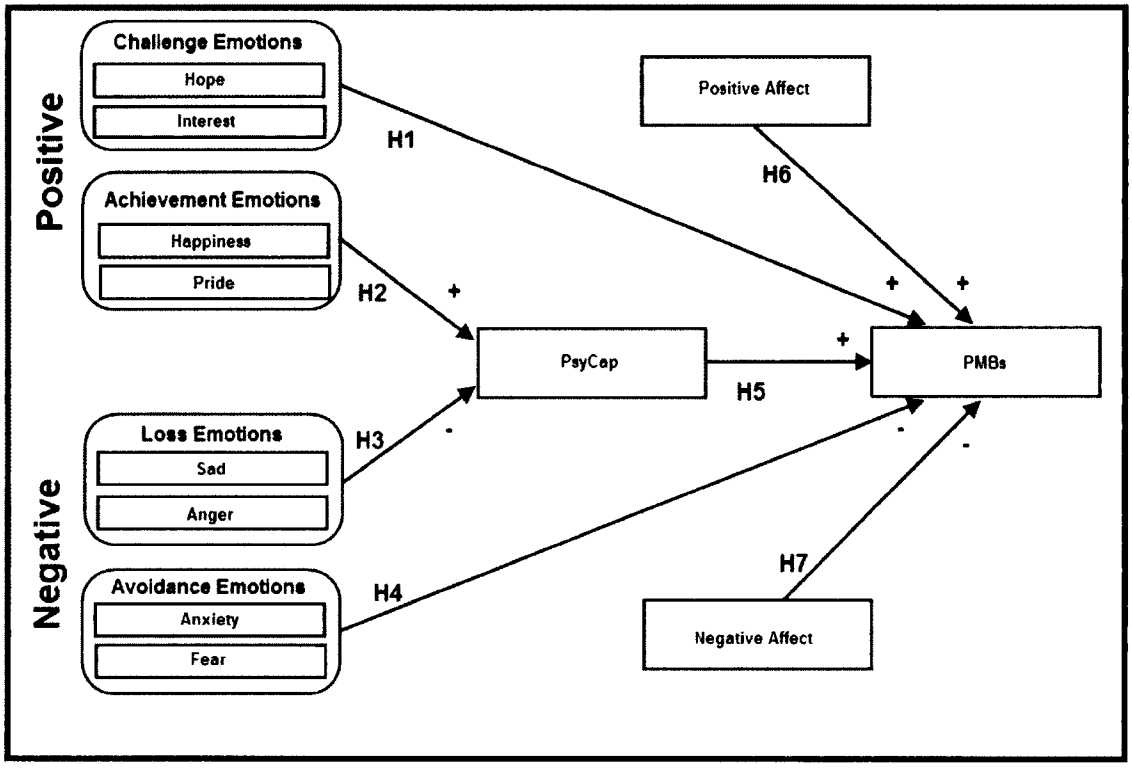


Figure 3.2 *Research Model*

Research Methodology

The multi-dimensional research model was tested empirically using survey research methodology. The instrumentation for the survey was developed based on a thorough literature review. Where possible, the items were adapted from prior research. All the items included in the final survey were subjected to subject matter expert review and were pilot tested before executing the final survey.

Study Measures

The first four hypotheses in the study ask respondents to report their emotional reaction to taking action against security threats to their organization. As in Beaudry and Pinsonneault (2010), I used Lazarus and Folkman's (1984) emotional intensity ratings to ascertain the emotional reaction to dealing with threats to the firm's security. Respondents were asked the following: "When you think about protecting your organization's information and information system from security threats, to what extent do you feel..." followed by indicators of discrete emotions from each quadrant of Beaudry and Pinsonneault's emotional framework. The indicators were adapted from Izard's (1977) differential emotions scale (DES) and Fredrickson's (2003) modified differential emotions scale (MDES) and measured *interest and hope* (Challenge), *happiness and pride* (Achievement), *anger and sadness* (Loss), and *fear and anxiety* (Avoidance). The measures of anxiety were taken from Venkatesh's (2000) measure of computer anxiety, which describes anxiety as making one feel nervous, threatened, bothered, uncomfortable, and uneasy.

PsyCap was measured using items adapted from the questionnaire developed by Luthans, Youssef et al. (2007b). The original PsyCap Questionnaire includes twenty-four items (six for each of the four characteristics). The PsyCap items were all developed from prior literature and have been executed successfully throughout the business literature. (Luthans et al., 2007a; Luthans et al., 2007b).

PsyCap Hope measures state-hope and is "responsive to events in the lives of people" (Snyder et al., 1996, p. 321). *PsyCap Hope* captures both the agency and pathway components of hope, and an example of an item measuring PsyCap Hope is "I can think of many ways to reach my current work goals"(Luthans et al., 2007b). *PsyCap Resilience* measures an individual's ability to bounce back or to take stressful things at work in stride (Wagnild et al., 1993). An example of an item measuring resilience is "I usually take stressful things at work in stride" (Luthans et al., 2007b). *PsyCap Optimism* measures an individual's state-belief that "good rather than bad things will happen to them" (Scheier et al., 1985, p. 219). An example of an item measuring *PsyCap Optimism* is "I approach this job as if 'every cloud has a silver lining'"(Luthans et al., 2007b). Lastly, *PsyCap Self-Efficacy* measures the state-like role-breadth self-efficacy and are based on Parker's (1998) self-efficacy scale. An example of an item measuring *PsyCap Self-Efficacy* is "I feel confident analyzing a long-term problem to find a solution" (Luthans et al., 2007b).

Positive affect and negative affect were measured in this study using the shortened positive affect/negative affect scale (PANAS) (Watson et al., 1988; Mackinnon et al., 1999). In order to capture general affectivity, the respondents were asked to "indicate to what extent you generally feel this way, that is how you feel on average."

The respondents rated a total of ten affect-related adjectives on a seven point likert scale, five reflecting positive affect and five reflecting negative affect.

Analysis and Results

The research model was analyzed in a two-step procedure as recommended by methodologists (Gerbing et al., 1988). The analysis utilized the covariance-based structural equation modeling (SEM) platform Mplus (Muthén et al., 1998-2010). In the first step, a confirmatory factor analysis (CFA) was run in Mplus to establish the validity of the measures to be included in the subsequent structural model. Upon confirmation of the validity of the research model, the hypothesized research model was assessed using Mplus. Prior to the collection of the data for the final analysis, the instrument was pilot tested to confirm the validity of the measures.

Instrument Development

Critical to any study is the validity and reliability of the measures employed (Straub, 1989; Gefen et al., 2011). As recommended, whenever possible the scales included in this study were employed as previously published (Straub et al., 2004). The instrument was assessed by subject matter experts and pilot tested with a convenience sample of ten organizational insiders. Upon completion of the survey instrument, the respondents in the pilot were directed to a separate form which allowed for feedback on the instrument. Based on these preliminary analyses, the survey instrument was deemed clear and appropriate.

Primary Study

After analyzing the results of the pretest and confirming the clarity of the instrumentation, responses were collected from a sample of 421 organizational insiders. Panels are especially appropriate for gathering security data as they offer full anonymity, not simply confidentiality. Given the sensitive nature of security responses, anonymity is required to encourage candid responses, and panels provide increased anonymity in multiple ways. First, the researchers never know the identity of the respondents, and the privacy of respondents is guaranteed and governed by the data provider. Second, respondents' real and perceived anonymity is enhanced by having access to the survey outside of their organization's network and computers. Providing anonymous, off-site access to self-report surveys has been shown to be adequate and appropriate for the elicitation of self-reported incidences of sensitive and even socially undesirable behaviors such as protection-motivated behaviors (Posey et al., 2013) and organizational deviance (Bennett et al., 2000; Bennett et al., 2003). The descriptive statistics of the primary sample are summarized in Table 3.3.

Table 3.3

Descriptive Statistics of Primary Sample

Average Age		44.62
Average Organizational Tenure		10.63
Gender	Female	53.7%
	Male	46.3%
Education	Some high school	9.7%
	High school diploma	17.6%
	Some college	13.5%
	Associate's or two-year degree	38.5%
	Undergraduate degree	15.4%
	Master's degree	4.8%
	Doctorate/Professional degree	0.5%
IT Position		14.5%
Management		33.0%

Construct Validity

For the reflective measures included in the structural model, the standardized factor loadings from a CFA analysis were considered along with the Cronbach's alphas. Also, the convergent and discriminant validity of measures in the structural model were assessed with average variance extracted (AVE) and the Fornell-Larker criterion (i.e., comparison of squared correlations with AVEs) as recommended by methodologists (Hair et al., 2006; Hair et al., 2014) (see Table 3.4).

Table 3.4

Full Measures in Study & Validity Statistics

Items	Measures	Scale[i]	Mean	STD	Load.
Challenge Emotions	"When you think about protecting your organization's information and information system from security threats, to what extent do you feel..."	Scale[i]	Mean	STD	Load.
Interest	Alert	c	3.86	1.78	0.764
	Curious	c	2.89	1.72	0.692
	Interested	c	3.67	1.78	0.872
Hope	Hopeful	c	3.37	1.83	0.847
	Optimistic	c	3.62	1.80	0.856
	Encouraged	c	3.49	1.81	0.911
Achievement Emotions	"When you think about protecting your organization's information and information system from security threats, to what extent do you feel..."	Scale[i]	Mean	STD	Load.
Happiness	Glad	c	3.54	1.95	0.925
	Happy	c	3.53	1.93	0.955
	Joyful	c	3.00	1.86	0.885
Pride	Proud	c	3.52	1.89	0.88
	Confident	c	4.10	1.73	0.89
	Self-assured	c	3.77	1.77	0.887
Loss Emotions	"When you think about protecting your organization's information and information system from security threats, to what extent do you feel..."	Scale[i]	Mean	STD	Load.
Anger	Angry	c	1.84	1.30	0.958
	Mad	c	1.81	1.25	0.946
	Annoyed	c	2.17	1.45	0.825
Sad	Sad	c	1.86	1.29	0.907
	Unhappy	c	1.92	1.33	0.904
	Discouraged	c	2.06	1.34	0.874
Avoidance Emotions	"When you think about protecting your organization's information and information system from security threats, to what extent do you feel..."	Scale[i]	Mean	STD	Load.
Fear	Scared	c	1.81	1.18	0.935
	Fearful	c	1.89	1.24	0.921
	Afraid	c	1.84	1.20	0.933

Table 3.4 (Continued)

Anxiety	Nervous	c	2.19	1.42	0.838
	Threatened	c	2.14	1.38	0.827
	Uneasy	c	2.16	1.40	0.888
PsyCap Hope (PCH)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Mean	STD	Load.
PCH-1	If I should find myself in a jam at work, I could think of many ways to get out of it.	a	5.40	1.07	0.687
PCH-2	At the present time, I am energetically pursuing my work goals.	a	5.15	1.30	0.803
PCH-3	There are lots of ways around any problem.	a	5.51	1.11	0.643
PCH-4	Right now I see myself as being pretty successful at work.	a	5.48	1.18	0.798
PCH-5	I can think of many ways to reach my current work goals.	a	5.38	1.12	0.771
PCH-6	At this time, I am meeting the work goals that I set for myself.	a	5.53	1.19	0.715
PsyCap Resilience (PCR)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Mean	STD	Load.
PCR-2	I usually manage difficulties one way or another at work.	a	5.59	0.99	0.79
PCR-3	I can be "on my own," so to speak, at work if I have to.	a	5.91	1.09	0.616
PCR-5	I can get through difficult times at work because I've experienced difficulty before.	a	5.54	1.05	0.724
PCR-6	I feel I can handle many things at a time at this job.	a	5.63	1.07	0.734
PsyCap Optimism (PCO)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Mean	STD	Load.
PCO-1	When things are uncertain for me at work, I usually expect the best.	a	4.57	1.36	0.738
PCO-3	I always look on the bright side of things regarding my job.	a	4.96	1.31	0.846
PCO-4	I'm optimistic about what will happen to me in the future as it pertains to work.	a	5.10	1.34	0.754

Table 3.4 (Continued)

PCO-6	I approach this job as if "every cloud has a silver lining."	a	4.86	1.27	0.788
PsyCap Self-Efficacy (PCSE)	(Luthans et al., 2007b) Instructions: "Please indicate your level of agreement with the following statements."	Scale	Mean	STD	Load.
PCE-1	I feel confident analyzing a long-term problem to find a solution.	a	5.43	1.18	0.816
PCE-2	I feel confident in representing my work area in meetings with management.	a	5.44	1.31	0.819
PCE-3	I feel confident contributing to discussions about the company's strategy.	a	5.09	1.42	0.791
PCE-4	I feel confident helping to set targets/goals in my work area.	a	5.44	1.24	0.811
PCE-5	I feel confident contacting people outside the company (e.g., suppliers, customers) to discuss problems.	a	5.18	1.46	0.736
PCE-6	I feel confident presenting information to a group of colleagues.	a	5.46	1.32	0.788
Protection Motivated Behaviors (PMB)	(Posey, 2010) Instructions: "Given the following statements, on what basis did you engage in the stated behaviors in the last year?"	Scale	Mean	STD	Load.
PMB-1	I actively attempted to protect my organization's information and computerized information systems	b	4.67	1.93	0.942
PMB-2	I tried to safeguard my organization's information and information systems from their information security threats	b	4.82	1.92	0.934
PMB-3	I took committed action to prevent information security threats to my firm's information and computer systems from being successful	b	4.44	1.99	0.891
PMB-4	I purposefully defended my organization from information security threats to its information and computerized information systems	b	4.42	1.99	0.923
PMB-5	I earnestly attempted to keep my organization's information and computer systems from harm produced by information security threats	b	4.80	1.92	0.92

Table 3.4 (Continued)

Positive Affect/ Negative Affect (PANAS)	(Mackinnon et al., 1999) Please indicate to what extent you generally feel this way, that is, how you feel on the average.	Scale	Mean	STD	Load.
Positive Affect (PA)	Enthusiastic	c	4.45	1.33	0.888
	Excited	c	4.03	1.29	0.811
	Alert	c	4.68	1.27	0.568
	Determined	c	4.90	1.33	0.684
	Inspired	c	4.19	1.43	0.848
Negative Affect (NA)	Nervous	c	2.61	1.28	0.771
	Distressed	c	2.45	1.25	0.786
	Upset	c	2.45	1.24	0.791
	Scared	c	2.06	1.15	0.823
	Afraid	c	2.07	1.15	0.824

(R) = reverse scored item

[i]Scale:

a) Strongly Disagree – Strongly Agree
b) Never – Always
c) Not at all – Completely

The CFA of lower-order constructs included in the study is characterized by strong fit with a Chi-Squared of 1857.50 with 1049 degrees of freedom (goodness of fit index: CFI = 0.944; badness of fit index: RMSEA = 0.043). As shown in Table 3.4, most of the standardized loadings of the reflective items were above a conservative 0.70 cutoff criterion. A loading of 0.70 indicates that the associated latent variable accounts for 50% of the variance in the indicator (Hair et al., 2006; Hair et al., 2014). The Cronbach's alpha of each construct was within the recommendations of prior research (Nunnally, 1978) (see Table 3.5).

Table 3.5

Lower-order Latent Variable Correlations

Chi-Squared = 1857.50; d.f.=1049 CFI=0.944; RMSEA=0.043																
	Hap.	Sad.	Pride	Ang.	Int.	Anx.	Fear	Hope	PMB	PCE	PCO	PCR	PCH	PA	NA	α
HAP.	**0.85**															0.94
SAD	0.02	**0.80**														0.92
PRIDE	0.78	-0.03	**0.78**													0.92
ANG.	-0.02	0.81	-0.04	**0.83**												0.93
INT.	0.67	0.18	0.76	0.14	**0.61**											0.81
ANX.	0.08	0.70	0.02	0.72	0.37	**0.73**										0.89
FEAR	0.04	0.71	-0.01	0.73	0.27	0.90	**0.86**									0.95
HOPE [1]	0.81	0.02	0.89	0.00	0.89	0.11	0.09	**0.76**								0.91
PMB	0.28	-0.04	0.37	-0.05	0.41	0.03	-0.05	0.42	**0.85**							0.97
PCE	0.25	-0.09	0.35	-0.07	0.37	-0.11	-0.09	0.33	0.36	**0.63**						0.91
PCO	0.26	-0.10	0.32	-0.05	0.29	-0.11	-0.11	0.36	0.38	0.64	**0.61**					0.73
PCR	0.16	-0.16	0.27	-0.18	0.34	-0.09	-0.18	0.29	0.30	0.67	0.67	**0.52**				0.81
PCH	0.27	-0.14	0.37	-0.11	0.32	-0.17	-0.14	0.35	0.31	0.89	0.70	0.73	**0.55**			0.88
PA	0.43	0.00	0.47	0.00	0.50	0.03	0.01	0.58	0.33	0.47	0.63	0.47	0.50	**0.59**		0.88
NA	0.06	0.41	-0.01	0.34	0.11	0.44	0.44	-0.02	-0.09	-0.23	-0.33	-0.33	-0.26	-0.14	**0.64**	0.90
***AVE's** bolded along diagonal																

[1] It should be noted that the discrete emotion 'hope' is distinct from the positive resource capability deemed 'PsyCap Hope'. Discrete emotion hope is a "mental state of readiness" with a specific referent—in this case protection of the firm's IS. This is supported by the strong correlations between discrete emotion 'hope' and challenge emotion 'interest' (r=0.89), relative to the correlation between discrete emotion 'hope' and 'PsyCap Hope' (r=0.35).

Each lower-order construct exhibits strong convergence and reliability. However, several of the first-order constructs are highly correlated with one another. High correlations among many of the constructs are theoretically supported in the literature such as the relationship between the facets of PsyCap. Further, as suggested by Beaudry and Pinsonneault's (2010) emotional framework, the emotions within each quadrant (i.e. achievement, loss, etc.) are highly correlated with one another as well. The lack of discrimination among the facets of PsyCap is appropriate as it is specified as a higher-order reflective construct. Construct specification is a topic of considerable interest in IS research, as the field seeks to employ second generation techniques with both theoretical and statistical validity (Bagozzi, 2011; Gefen et al., 2000; Gefen et al., 2011; Straub et al., 2004; Jarvis et al., 2003). Constructs defined as first- and second-order reflective appear most often in business research (Jarvis et al., 2003), and specify that the indicators at each level "reflect" the latent variable (Straub et al., 2004; Jarvis et al., 2012).

For the discrete emotions within each quadrant of the emotional framework, however, it is inappropriate to specify them as second order characteristics as fundamental to the very nature of discrete emotions is their distinction (DeSteno et al., 2004). Further, a primary objective of this study is to examine the impact of discrete emotions from each quadrant of the emotional framework on the protection of organizational resources. Therefore, in order to examine the hypotheses in this study, two structural models were ultimately examined. As shown in Figure 3.3, each model has a unique discrete emotion from the four quadrants of the emotional framework. All constructs in each model exhibit convergence and discriminance as indicated by the ratio of Fornell-Larker statistic and latent variable correlations of ≤ 1.

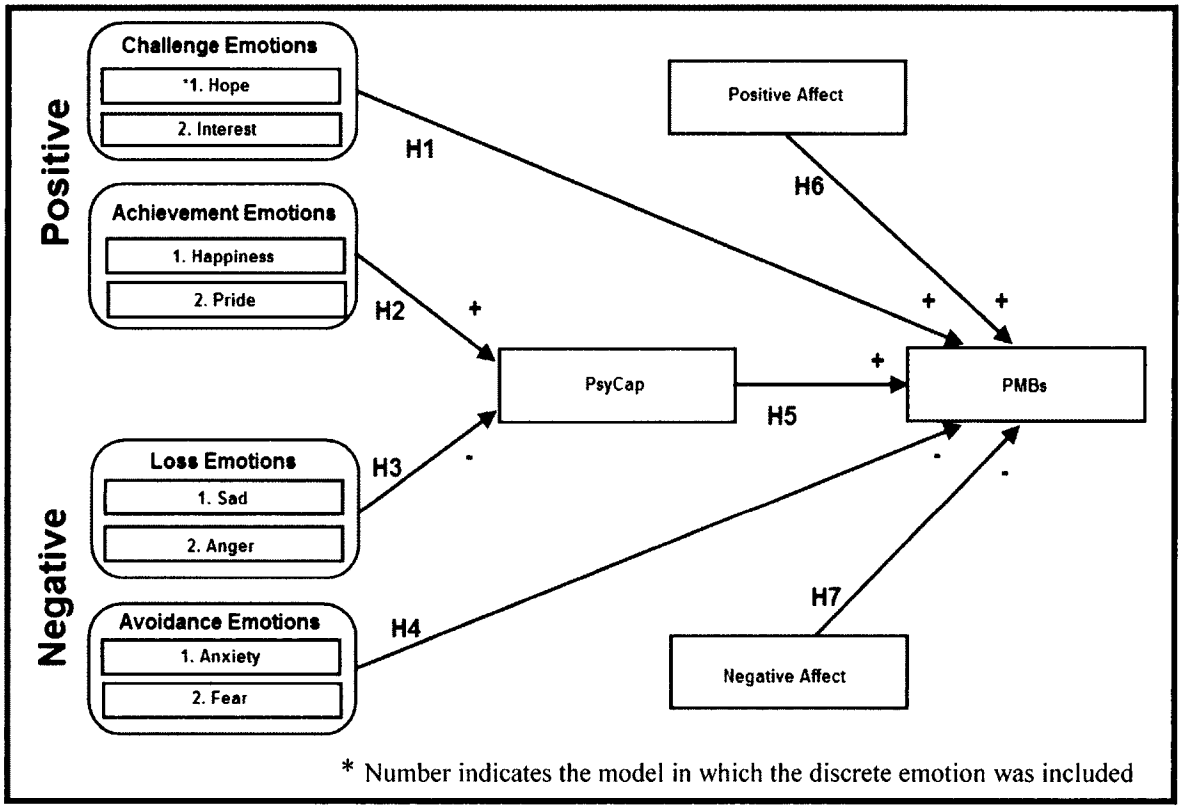


Figure 3.3 *Research Model*

Structural Model

Finally, the hypothesized relationships in the research model were tested using SEM. For model one, the Chi-Squared statistic and degrees of freedom (X^2=2015.84 and d.f.=1008; X^2 to d.f. ratio = 2.0) along with a goodness of fit index (CFI =0.93) and a badness of fit index (RMSEA=.049) all indicate that the structural model has good fit overall (Hu et al., 1999; Kline, 2010). Further, four of seven hypothesized relationships are significant and in the predicted direction. (see Table 3.6.)

Table 3.6

Structural Model Results – Model 1

Chi-Squared = 2015.84; d.f.= 1008 CFI=0.934; RMSEA=0.049				
Hyp.	Hypothesis (direction)	Path Coefficient	p-value (one-tailed)	Significance (one-tailed)
H1	**Hope → PMBs (+)**	**0.306**	**<0.001**	***
H2	**Happiness → PsyCap (+)**	**0.292**	**<0.001**	***
H3	**Sadness → PsyCap (-)**	**-0.149**	**0.002**	**
H4	Anxiety → PMBs (-)	0.051	0.173	n/s
H5	**PsyCap → PMBs (+)**	**0.245**	**<0.001**	***
H6	Positive Affect → PMBs (+)	0.021	0.376	n/s
H7	Negative Affect → PMBs (-)	-0.045	0.208	n/s
Dependent Variable R Square				
R^2	**PMB**	**0.203**	**<0.001**	***
Bold = supported; *p=0.05; **p=0.01; ***p=0.001; n/s=not significant				

For model two, the Chi-Squared statistic and degrees of freedom (X^2=2052.36 and d.f.=1008; X^2 to d.f. ratio = 2.04) along with a goodness of fit index (CFI =0.93) and a badness of fit index (RMSEA=.05) all indicate that the structural model has good fit overall (Hu et al., 1999; Kline, 2010). Additionally, five of the seven hypothesized relationships are significant and in the predicted direction. (see Table 3.7.)

Table 3.7

Structural Model Results – Model 2

Chi-Squared = 2052.36; d.f.= 1008 CFI=0.932; RMSEA=0.05				
Hyp.	Hypothesis (direction)	Path Coefficient	p-value (one-tailed)	Significance (one-tailed)
H1	**Interest → PMBs (+)**	**0.344**	**<0.001**	***
H2	**Pride → PsyCap (+)**	**0.402**	**<0.001**	***
H3	**Anger → PsyCap (-)**	**-0.101**	**0.019**	*
H4	**Fear → PMBs (-)**	**-0.100**	**0.033**	*
H5	**PsyCap → PMBs (+)**	**0.204**	**<0.001**	***
H6	Positive Affect → PMBs (+)	0.049	0.217	n/s
H7	Negative Affect → PMBs (-)	-0.025	0.325	n/s
Dependent Variable R-Square				
R^2	**PMB**	**0.220**	**<0.001**	***
Bold = supported; *p=0.05; **p=0.01; ***p=0.001; n/s=not significant				

Controls and Rival Explanations

To substantiate the findings of the structural model, the analyses were performed again including several controls. As can be seen in Table 3.8, controls for age, tenure, gender, and social desirability had no significant impact on the performance of PMBs. Conversely, whether or not an insider was a manager or an IT staffer did have a significantly positive relationship with performance of PMBs. Further, level of education completed as well as frequency of organizational SETA programs were also significantly positively related to the performance of PMBs. Importantly, the significance and direction of all substantive variables remained consistent while controlling for these plethora of insider characteristics (see Table 3.8, Figures 3.4, and 3.5).

Table 3.8

Structural Model Results Including Controls

		Model 1		Model 2	
Hyp.	Hypothesis (direction)	Path Coefficient	Significance (one-tailed)	Path Coefficient	Significance (one-tailed)
H1	**Hope → PMBs (+)**	**0.218**	***		
H1	**Interest → PMBs (+)**			**0.246**	***
H2	**Happiness → PsyCap (+)**	**0.291**	***		
H2	**Pride → PsyCap (+)**			**0.403**	***
H3	**Sadness → PsyCap (-)**	**-0.150**	**		
H3	**Anger → PsyCap (-)**			**-0.101**	*
H4	Anxiety → PMBs (-)	0.016	n/s		
H4	**Fear → PMBs (-)**			**-0.105**	*
H5	**PsyCap → PMBs (+)**	**0.194**	***	**0.164**	**
H6	Positive Affect → PMBs (+)	0.045	n/s	0.049	n/s
H7	Negative Affect → PMBs (-)	-0.025	n/s	-0.024	n/s
Controls					
	Age	0.012	n/s	0.011	n/s
	Tenure	0.011	n/s	0.012	n/s
	Manager	0.076	*	0.079	*
	IT Position	0.153	***	0.148	***
	Gender	-0.013	n/s	-0.007	n/s
	Education	0.116	**	0.126	**
	SETA	0.243	***	0.235	***
	Social Desirability	0.078	n/s	0.075	n/s
Dependent Variable R-Square					
R^2	**PMB**	**0.262**	***	**0.276**	***
Bold = supported; *p=0.05; **p=0.01; ***p=0.001; n/s=not significant					

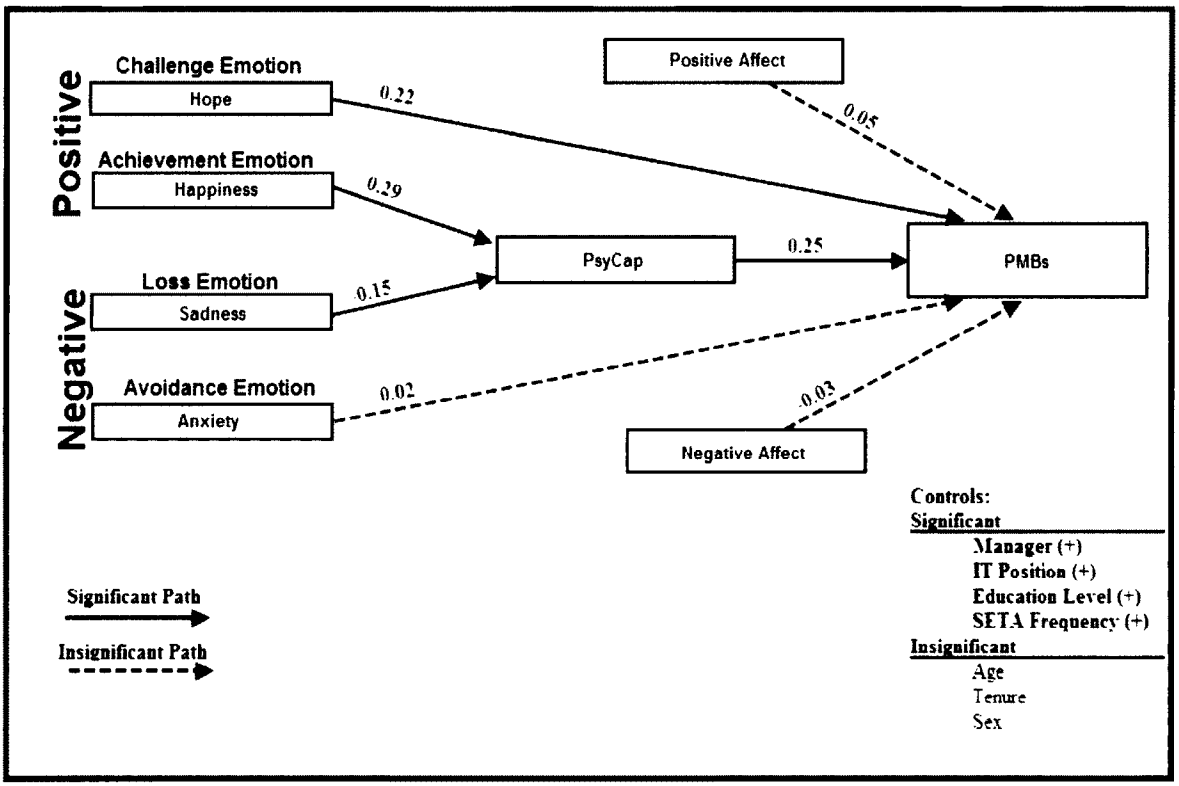


Figure 3.4 *Model 1 Results*

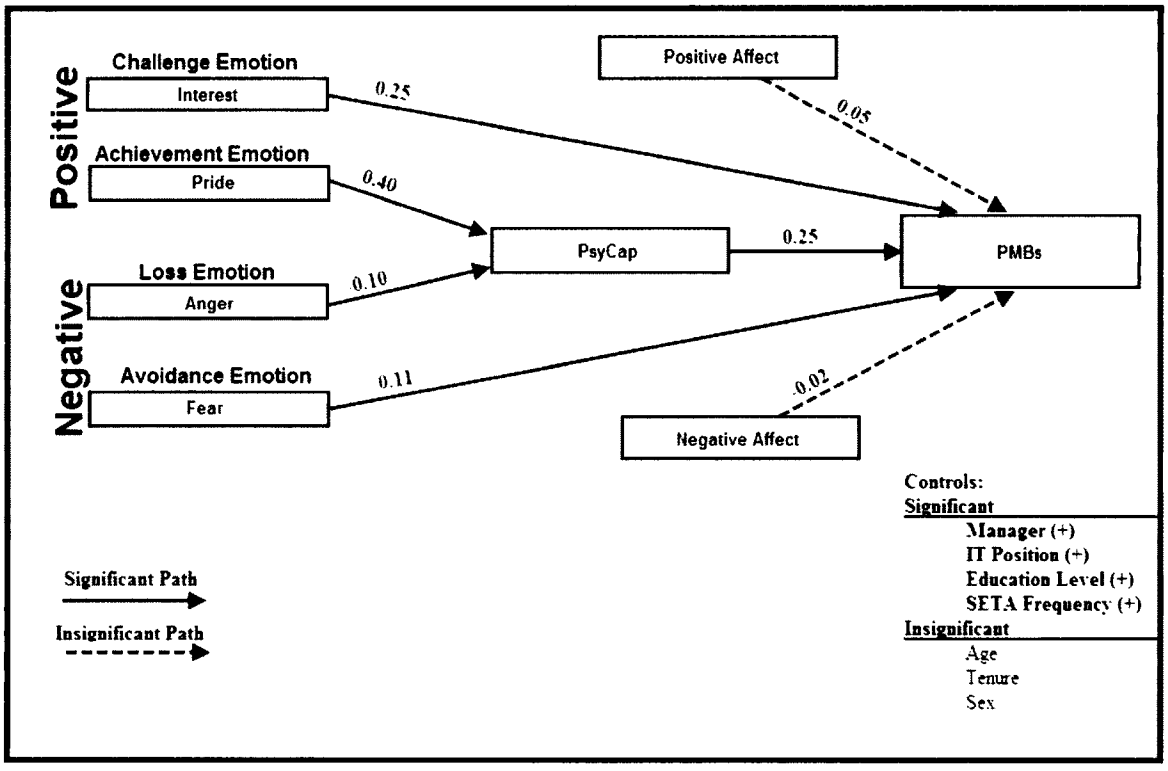


Figure 3.5 *Model 2 Results*

Discussion

The results of the analyses provide support for the broaden-and-build theory of positive emotions. First, in line with the 'broaden' hypothesis of broaden-and-build model, discrete challenge emotions of 'hope' and 'interest' were both significantly and positively related to the performance of PMBs. Second, in support of the 'build' hypothesis, discrete achievement emotions of happiness and pride were positively and significantly related to PsyCap in both models.

Implicit in the broaden-and-build theory of positive emotions is an inverse relationship between negative emotions and personal outcomes. That is, there is also both an implied 'narrowing' and 'taxing' hypothesis. The 'taxing' hypothesis was supported in both models as the loss emotions of sadness and anger were both negatively related to insiders' PsyCap. The 'narrowing' hypothesis received mixed support, with the discrete emotion 'fear' negatively relating to PMBs, and 'anxiety' failing to relate significantly to PMBs.

Insiders' PsyCap was positively related to the performance of PMBs in both models. Additionally, the stable personality characteristics of positive affect and negative affect were not significantly related to PMBs in either model. Finally, the model was robust to a plethora of controls. Supporting the stability of the model of security emotion, the significance and magnitude of the controls were consistent across models. In both models, controls for management, IT position, level of education, and SETA frequency were significantly related to PMBs. Conversely, organizational tenure, age, and gender were not significantly related to PMBs.

Implications and Contributions

This research makes important contributions to the behavioral information security literature. Principally, the results impart the significant and diverse impact that emotions play in the performance of protective behaviors. The broaden-and-build model provides a framework of the disparate impact of discrete positive and negative emotions on both insiders' behavioral tendencies and psychological resources. The importance of emotion to security is made manifest in the found direct and indirect influences of emotional experience on insiders' performance of PMBs.

Complementary to the broaden-and-build theory, this research goes further and applies Beaudry and Pinsonneault's (2010) framework of emotions to the broaden-and-build model to ascertain the importance of specific action tendencies of four categories of emotions (challenge, achievement, loss, and avoidance). The results largely support the classification of emotions according to specific action tendencies (as in Beaudry and Pinsonneault's framework). In addition to similarities shared among the quadrants of the emotional framework, the results also support nuance among the discrete emotions, even those which generally share the same specific action tendency (i.e. from the same quadrant). Each emotion plays a unique role in the elicitation of PMBs and the building of insiders' PsyCap. For instance, interest was more strongly related to PMBs than hope, and pride more strongly related to PsyCap than happiness. Interestingly, fear was negatively related to PMBs, while anxiety had no significant relationship.

The findings provide research with an alternative view to the often negative appeal to emotion (i.e. fear appeals) employed in security research (e.g. Johnston et al., 2010). The research model elucidates the efficacy of emotional appeals as relating to the

specific action tendencies associated with the underlying discrete emotion. While the action tendencies related to emotion are often considered to be evolved or innate, the elicitation of emotion can be manipulated through conditioning. Further, emotional stimuli result from adaptational encounters (Lazarus, 1991). This research ascertained insiders' emotional reaction to protecting their firm from security threats, rather than their response to the threats themselves. This distinction is important as it appropriately measures emotion in response to an encounter rather than an object and explains a negative relationship between fear and PMBs.

Organizations and researchers recognize the benefit of emotional reactions; however, as shown in the current study the referent of the emotion is significant. Therefore, the security benefit provided by fear appeals may be confounded or diminished if the fear is elicited in terms of actually protecting the firm. Further, the research exhibits the significant role that positive emotions can play in increasing security of an organization. Insiders who feel hopeful and interested when thinking about protecting their firm from security threats were more likely to engage in PMBs.

In addition to the direct impact of challenge and avoidance emotions, achievement and loss emotions were found to indirectly impact the performance of PMBs through the building (or taxing) of the positive psychological resource of PsyCap. PsyCap is related to myriad positive organizational and personal outcomes and is also linked in this research to the performance of PMBs. Both achievement emotions: pride and happiness, were shown to relate positively to insiders' PsyCap, while loss emotions were a tax on insiders' PsyCap.

Finally, the more stable characteristics of positive and negative affect were not related to the performance of PMBs. The insignificant effect of positive affect and negative affect (PANA) in this model is important for two reasons. First, the inclusion of PANA serves as an important control for the effect of discrete emotions. Second, general affect is not readily manipulated by an organization. Unlike discrete emotions, general affect is not the result of specific stimuli, but rather a measure of the general experience of emotion of an individual. Therefore, the finding that insider mood is not a significant predictor of PMBs allows organizations to focus on manipulation of emotional response to security-related stimuli rather than the screening employees for general affectivity (see Table 3.9).

Table 3.9

Summary of Key Findings

Key finding	**Significance to research**	**Significance to practice**
Support for the broaden-and-build model of positive emotions in behavioral information security.	Broadens the theoretical repertoire of behavioral information security research to include a positive security paradigm incorporating the security contribution of positive emotions.	Provides organizations with a framework within which to manipulate insiders' positive emotional reaction to security-related stimuli.
Support for the disparate impact of discrete emotions within Beaudry and Pinsonneault's emotional framework	Establishes the diverse impact of discrete emotions on the performance of security-related behaviors based on specific action tendencies of categories of emotions.	Provides organizations with an emotional schema for eliciting security-related behaviors based on the experience of discrete emotion in response to specific security-related stimuli.

Table 3.9 (Continued)

Negative influence of the avoidance emotion fear on PMBs.	Provides evidence of the potentially confounding or diminishing effect of the experience of fear on the performance of PMBs based on the elicitation of avoidance emotions in response to protection of the firm.	Highlights the potential shortcoming of fear appeals on the elicitation of security-related behaviors based on the distinction between fear response to a threat and fear response to protecting the firm.
Influence of achievement and loss on PsyCap	Establishes the relationship between the experience of emotion in response to security-related stimuli and the positive resource capabilities of insiders and myriad other positive organizational outcomes	Provides organizations with a link between emotion and insider's PsyCap and the many positive organizational outcomes associated with PsyCap.
Influence of PsyCap on PMBs	Evidences a direct link between PsyCap and organizational security for future research.	Further establishes the positive personal and organizational outcomes attributable to PsyCap
No significant relationship between PANA and PMBs.	Acts as an important control for the establishment of the role of discrete emotion in behavioral information security.	Provides support for organizational influence on security outcomes from stimuli induced discrete emotion and removes the burden of screening for general affect when seeking to elicit PMBs from insiders.

Limitations and Future Research

There are inherent limitations in self-reported security research, and to a large extent this research is no exception. However, due to the absence of observational data of actual security behaviors, survey instruments are an accepted medium for ascertaining the behavior of insiders. I took recommended precaution to ensure that individual anonymity was preserved and responses were uninhibited. The data analyzed in this research was

collected at a cross-sectional level with differences measured between randomly surveyed organizational insiders. The research model ascertained the impact of discrete emotion on security-related behavior. The researcher's inability to capture emotional responses from insiders in an experimental setting creates an additional limitation. Due to the difficulty in recalling past emotions, the instrument asked insiders to respond how they feel when they think about protecting their organization from security threats, eliminating the temporal disparity between the experience and the survey response.

The results highlight several important avenues of future security research as well. First, the results support the expansion of the theoretical repertoire to include adaptational approaches to security-related behavior such as the broaden-and-build theory. Second, the results highlight the need for future research into the impact of positive emotions in behavioral information security and IS at large. Additionally, the research model exhibits an important relationship between security and insiders' PsyCap. As shown, an insider's emotional reaction to security had a significant impact on insiders' PsyCap, and PsyCap is positively related to PMBs. In the same way, this research links positive security outcomes to other positive personal and organizational outcomes previously associated with PsyCap. Finally, the research highlights the need for future research into the discrete emotions which impact security. As can be seen, the emotional framework provides an important categorization of emotion; however, each discrete emotion retains unique influence as well.

Conclusion

This chapter developed and applied a research model based on the broaden-and-build theory while incorporating the classification of emotions provided in Beaudry and

Pinsonneault's framework of emotions. The results of the study indicate that discrete emotions are impactful on the performance of PMBs. The results support the concept specific action tendencies espoused in an adaptational view of emotions while simultaneously confirming the nuance between discrete emotions. The elicitation of challenge emotions in the protection of the firm stimulated PMBs in both models, while the elicitation of avoidance emotions had mixed results. The experience of fear when protecting the firm was negatively related to PMBs and anxiety had no relationship.

The results of the research models tested also support the stated and implied 'building' and 'taxing' role of emotions on personal resources. Achievement emotions were positively related to PsyCap, while loss emotions were negatively related. These emotions are indirectly related to PMBs as PsyCap was significantly related to the performance of PMBs. The influence of PsyCap on PMBs adds to the myriad of positive personal and organizational outcomes previously attributed to PsyCap in the organizational literature. Lastly, positive and negative affect were unrelated to the performance of PMBs. This lack of influence of PANA provides an important control for the influence of discrete emotion. Additionally, as PANA captures general disposition, its lack of significance highlights the importance of investigating the impact of discrete emotions elicited by security-related disposition as opposed to general affectivity.

CHAPTER 4

SECURITY BEHAVIORAL COMPLEXITY AND PSYCHOLOGICAL CAPITAL: AN EMPIRICAL EXAMINATION

Introduction

The digital age has ushered in a dynamic environment of rapid innovation and ubiquitous computing. The repercussions are global, as corporate mobile device usage has reached the "tipping point" with 50% of organizations worldwide allowing employees to use mobile devices for tasks such as sales force automation, project management, and email (Symantec, 2012). Recent surveys in the U.K. and Canada indicate that employees access email and corporate documents from personal devices at an increasing rate—often without oversight from their employer (CDW, 2013; Wilson, 2013). Additionally, 54% of U.S. based organizations report an inability to determine if off-site employees are using technology and informational resources within corporate and regulatory requirements (Ponemon, 2013). In this connected environment, many practitioners and academicians recognize that the information security of most firms is largely at the mercy of those with access to the firm's information and information system (IS) (Moore et al., 2008; Boss et al., 2009; D'Arcy et al., 2007). This revelation—fueled by frequent reportage of data breaches—has rightfully led to copious articles warning of the *threat of the insider* (e.g. Shaw et al., 1998; Boss et al., 2009; Vroom et al., 2004; Willison et al., 2009; Greitzer et al., 2008). Users have even been declared the

"weakest link" in IS security (Sasse et al., 2001). Fortunately, however, within the greatest weakness often lies the greatest opportunity (Albrechtsen et al., 2009; Stanton et al., 2005; Posey et al., 2013).

Evidence of insider's beneficial security behaviors has been presented in prior research, ranging from basic security hygiene (Stanton et al., 2005) to policy compliance (Pahnila et al., 2007; Siponen et al., 2006; Herath et al., 2009). Providing a definitive framework, Posey et al. (2013) systematically identified security roles—which they call protection-motivated behaviors (PMBs)—that can be enacted by employees to transform insiders from a security-related liability into an asset. *PMBs* are the volitional behaviors organizational insiders can enact to protect (1) organizationally relevant information within their firms and (2) the computer-based IS in which that information is stored, collected, disseminated, and/or manipulated from information-security threats (Posey et al., 2013). *Organizational insiders* are all individuals (e.g., full- and part-time employees, temporary workers, consultants, board members) who have access to organizationally relevant information while fulfilling their duties (Posey et al., 2013; Shaw et al., 1998). Therefore, in order to most effectively secure the organization's sensitive information and IS, insiders should incorporate PMBs into their behavior and actively work toward the protection of informational resources.

PMBs are roles that may be unrelated to or even in direct contrast with an insider's formal job description. PMBs are enacted alongside the various organizational roles held by all insiders with access to informational resources, creating behavioral complexity for insiders (Posey et al., 2013). *Behavioral complexity* refers to "the ability to act and play multiple roles that call for diverse and even competing behaviors" (Wu et

al., 2010, p. 818). Hooijberg (1996) established that behavioral complexity is comprised of two distinct components: (1) behavioral repertoire and (2) differentiation. *Behavioral repertoire* is the portfolio of roles an individual performs and his or her ability to perform multiple roles, and *differentiation* is the ability to "switch from role to role at appropriate times to handle paradoxes and contradictions mandated by one's job" (Wu et al., 2010, p. 818).

PMBs are manifest in a security behavioral repertoire, which is distinct to each insider (i.e. each user has his or her own unique repertoire of behaviors to draw upon) and are enacted across employees according to his or her ability to switch between roles. This phenomenon is *security behavioral complexity* and is defined as an insider's security behavioral security behavioral repertoire–paired with his or her differentiation (Wu et al., 2010; Hooijberg, 1996). Security behavioral complexity offers insight into what has become known as the "knowing-doing" gap of security behaviors in which employees fail to enact known behaviors to protect the organization's information and IS (Workman et al., 2008).

An individual's security behavioral repertoire can be thought of as a set of behavioral resources from which the individual may draw. In addition to behavioral resources, many theorists argue that effective adaptation is also dependent upon the psychological resources of the actor (e.g. Hobfoll, 1989; Hobfoll, 2002). One related conceptualization of personal resources comes from recent work in positive psychology: psychological capital (PsyCap) (Luthans et al., 2007a; Luthans et al., 2007b). *Positive psychology* can be described as "the study of the conditions and processes that contribute to the flourishing or optimal functioning of people, groups, and institutions" (Gable et al.,

2005, p. 103), and *PsyCap* is a construct of positive "psychological resource capabilities" which are open to development (Luthans et al., 2009).

Behavioral complexity has recently been espoused as an antecedent to the performance of PMBs (Posey et al., 2013), but has yet to be empirically examined. In light of this gap, I develop and empirically test a model of behavioral security complexity, which considers the impact of security behavioral complexity and PsyCap simultaneously.

Background

Decades ago, Straub and Nance (1990) predicted that the security-related impact of insiders would steadily increase over the years as average employees gain increased computing ability through their use of personal computers (PCs). This prediction has proven to be prophetic as widespread computer use has not only come to fruition, but has largely been eclipsed by the astounding penetration of the Internet. Pew Research Center reports that in the U.S. 78% of all adults are now online, up from just 10% in 1995 (Zickuhr et al., 2012). Paralleling this rise of access and ability of insiders has been the interest in behavioral information security. *Behavioral information security* is the study of "the human actions that influence the availability, confidentiality, and integrity of information systems" (Stanton et al., 2006b, p. 263).

Today, the prevailing market is largely a knowledge economy in which intellectual assets are a firm's most valuable resources (Johnson et al., 2009). Therefore, employees most often have the greatest access to their firm's "crown jewels" (Stanton et al., 2006a). The security of a firm's informational assets requires that firms incorporate a holistic approach to security (Lee et al., 2002): incorporating up-to-date technical security

mechanisms (Zafar et al., 2009), deterring detrimental behavior (e.g. computer abuse - Straub et al., 1990; Johnston et al., 2010; D'Arcy et al., 2012), and promoting protective behaviors (e.g. PMBs - Posey et al., 2013). The implementation of these diverse protections leads to the emergence of behavioral complexity for insiders (Posey et al., 2013).

Security Behavioral Complexity

Behavioral complexity implies a confrontation with paradox (Posey et al., 2013; Smith et al., 2011; Wu et al., 2010). Behavioral complexity—paired with cognitive complexity and psychological resources—has been espoused to provide an individual with the ability to "accept paradoxical tensions rather than respond defensively" (Smith et al., 2011). Cognitive complexity refers to the ability to process stimuli in order to undertake adaptation (Kiesler et al., 1982). Therefore, cognitive complexity can be regarded as a *necessary* condition for handling complexity, while behavioral complexity is the *sufficient* condition (Denison et al., 1995). Wu et al. (2010, p. 818) note "behavioral complexity is the manifestation of cognitive complexity that we can observe, evaluate and benchmark." Behavioral complexity is an important characteristic of individuals charged with enacting complex and/or paradoxical roles and serves as an appropriate proxy for *both* cognitive and behavioral complexity. Posey et al. (2013) note, the concept of behavioral complexity enables researchers and practitioners to "explain, motivate, and manage PMBs properly." A primary goal of this study is to introduce a model of security behavioral complexity into behavioral information security that provides a robust framework within which to examine the enactment of PMBs.

Security Behavioral Repertoire

An individual's behavioral repertoire represents the portfolio of roles which an individual is able to enact (Hooijberg, 1996; Wu et al., 2010). Behavioral repertoire may also represent a domain specific collection of roles—such as PMBs (Posey et al., 2013). Posey et al.'s (2013) taxonomy of PMBs provides a systematic-based classification of the security roles which make up the protective behaviors which an individual may have in his or her security behavioral repertoire. Therefore, *security behavioral repertoire* is defined as the collection of protective security behaviors (i.e. PMBs) which an insider is able to perform.

As implied in a model of security behavioral complexity and confirmed in the taxonomy of PMBs, robust protection of the firm's informational assets and systems requires that insiders hold various security roles within their security behavioral repertoire. This view is unique to much extant security research which has focused on singular behaviors such as anti-malware or anti-spyware software adoption (e.g. Lee et al., 2009; Johnston et al., 2010) or compliance with formalized security polices (e.g. Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath et al., 2009; Vroom et al., 2004). Policy compliance is an important goal of any organization, but—as a subject of empirical research—investigations of motivation and/or intention to comply with security policy often fail to capture the ability to undertake the protective behaviors themselves. An insiders' security behavioral repertoire includes not only an insiders' awareness of policy, but views the ability to comply with policy as a part of a larger behavioral repertoire. Additionally, software solutions are most often adopted by the IT department rather than the ordinary users of the system. Therefore, implementation of security software best

reflects an organization's investment in IT security rather than the motivation of insiders' to protect the organization (Kumar et al., 2008; August et al., 2006).

Security research has also relied on general perceptions of behavioral self-efficacy as opposed to the more specific security behavioral repertoire (Herath et al., 2009; Bulgurcu et al., 2010; Johnston et al., 2010; Boss et al., 2009; Lee et al., 2009; Workman et al., 2008; Woon et al., 2005). Many of the identified roles which emerged from the newly developed taxonomy of PMBs have been examined in one form or another in past research; however, security research has largely lacked the comprehensiveness offered by a behavior complexity model (Zafar et al., 2009). For example, the protection of organizational resources has been examined in terms of "values of people" (Dhillon et al., 2006), organizational climate (Chan et al., 2005), and even "social censure" (D'Arcy et al., 2011), yet a research framework for assessing behavioral roles in concert with the other implied roles of information security has yet to be established. Incorporating consideration of the breadth and magnitude of insiders' security behavioral repertoire into the research allows researchers to examine the ability to take on security roles across the entire domain of protective behaviors (e.g. PMBs) simultaneously.

Though prior research has made great strides in ascertaining the conditions of and antecedents to information security, the knowing-doing gap persists (Workman et al., 2008). Behavioral complexity allows for an examination of the impact of insiders' behavioral repertoire along with the complementary differentiation.

Security Differentiation

Differentiation is the ability to switch roles as demanded by the situation (Wu et al., 2010; Hooijberg, 1996). Differentiation implies an improvisational view of behavior,

incorporating behavioral diversity in a dynamic environment. The dynamism and interrelatedness of organizational behavior has led to anthropomorphic and metaphorical descriptions for explanation. Drucker (2012) introduced a musical metaphor, analogizing the role of manager to that of an orchestral conductor. Yet, according to Drucker, "neither business nor government agency has a 'score' to play by" (Drucker, 2012 loc.3051-3052). Much like a jazz musician's ability to fluctuate between solos and melodies, tempos and time signatures, *security differentiation* is an insider's ability to switch between the various security behaviors incorporated in one's security behavioral repertoire (Wu et al., 2010; Posey et al., 2013). The jazz metaphor is instructive because the players enact their skills not in a vacuum, but rather incorporate their repertoire of abilities into a dynamic, spontaneous composition (Barrett, 1998).

Many insiders must safeguard both the sensitive information they have in their possession as well as their access to the organization's information system on an ongoing basis (Ayyagari et al., 2011). Each task and environment is characterized by unique security requirements, and consequently the effectiveness of the protective response is reliant upon the insiders' security differentiation. *Security differentiation* is the ability of an insider to effectively switch from one security role to another along the course of his or her work and is a core component of the security behavioral complexity model (Posey et al., 2013). Abilities such as those conceptualized by security behavioral complexity may be necessary but insufficient conditions of behavior, however, as behavior is a function of personal resources as well (Hobfoll, 2002).

Psychological Capital

Hobfoll (1989) posits that individual's draw on personal psychological resources in order to maintain resilience in the face of adversity. Similarly, it has been postulated that personal characteristics such as equanimity equip one to deal with the tensions of divergent demands (Smith et al., 2011). *Equanimity* is a facet of resilience which characterizes one who maintains a balanced perspective, and *resilience* "connotes inner strength, competence, optimism, flexibility, and the ability to cope effectively when faced with adversity" (Wagnild, 2009, p. 105). Positive psychological resources such as resilience have received greater consideration as a result of the growing positive psychology movement (Luthans et al., 2006b; Seligman et al., 2000). Positive psychology has as its domain "optimal functioning" or what is referred to in positive psychology literature as "flourishing" (Seligman et al., 2000). From this focus on optimal functioning, PsyCap has emerged as a construct of positive "psychological resource capabilities" which are open to development (Luthans et al., 2009).

As a higher order construct, PsyCap is composed of the distinct—yet related—core tenets of positive psychology of hope, resilience, optimism, and self-efficacy. Positive psychology is uniquely able to contribute to the current behavioral security research because it has the "average person" as its subject (Sheldon et al., 2001). In addition, PsyCap has received broad acceptance in business research and beyond (Avey et al., 2009; Walumbwa et al., 2011; Avey et al., 2010; Peterson et al., 2011), and has been linked to a number of positive personal and organizational outcomes such as job performance and satisfaction (Luthans et al., 2007a), low absenteeism (Avey et al., 2006),

low turnover and stress (Avey et al., 2009), as well as increased citizenship and decreased deviance (Avey et al., 2011).

PsyCap hope can be defined as a "positive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287; Luthans et al., 2007a). *PsyCap resilience* "is characterized by positive coping and adaptation in the face of significant risk or adversity" (Luthans et al., 2007a, p. 546; Masten, 2001; Masten et al., 2002). Resilience can also be thought of simply as "the positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702; Luthans et al., 2007a). *PsyCap optimism* is defined as that characteristic that is held by individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985). *PsyCap self-efficacy* is role-breadth self-efficacy and is defined as "the employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66; Luthans et al., 2007a).

PsyCap can be viewed through a resource lens (Luthans et al., 2007b; Hobfoll, 1989; Hobfoll, 2002). Hobfoll (1989) stipulates that individuals require resources for functioning, and they will seek to gain available resources and when possible conserve unnecessarily expended resources. Thus, the conservation of resources theory has two components: building up of resources and conservation of resources. PsyCap as a resource can be built by either micro-intervention or by macro-intervention such as a

supportive climate (Luthans et al., 2008). In reference to conservation, resources are either "centrally valued in their own right" or "as a means to obtain centrally valued ends" (Hobfoll, 2002). PsyCap can be viewed as adaptive in that not only does PsyCap embody a positive psychological state, as a psychological construct it serves meaningful ends. For instance, PsyCap has been shown to provide a necessary psychological resource for psychological well-being (Culbertson et al., 2010).

A distinguishing quality of PsyCap and perhaps one reason that it has been so widely considered is that it has been shown to be composed of characteristics that are state-like rather than trait-like. Though research has often relied on context to inform the true distinction between state and trait (Allen et al., 1981), there is an important distinction to be made between trait-like and state-like dispositions (Zuckerman, 1983; Fugate et al., 2012). This distinction is important as it differentiates those characteristics which are innate and inflexible from those which are malleable and developable. Trainable characteristics are especially critical in a security context because they can be developed within an organization to enhance organizational security. PsyCap is a construct composed of state-like characteristic and has been shown to be developable (Luthans et al., 2007a; Luthans et al., 2006a; Peterson et al., 2011). Therefore, any benefits to firm security which can be shown to be attributable to PsyCap can be influenced by an organization through an "investment" in employees' PsyCap. This ductile quality of PsyCap distinguishes it from other, more stable, traits like "The Big Five" personality traits (Goldberg, 1990) and the higher order "Core Self-Evaluation" (Judge et al., 2001; Luthans et al., 2007a). Peterson (2012) notes:

> "People's locus of control and self-esteem are things a manager probably can't change significantly within a few weeks. Psychological capital is

more malleable. We're not born hopeful, resilient, optimistic, efficacious people. We learn these things."

The facets of PsyCap and established facet-level development strategies are summarized in Table 4.1.

Table 4.1

Summary of PsyCap Characteristics

PsyCap Component	Definition	Micro-Development
PsyCap Self-Efficacy	"[T]he employee's conviction or confidence about his or her abilities to mobilize the motivation, cognitive resources or courses of action needed to successfully execute a specific task within a given context" (Stajkovic et al., 1998, p. 66)	• Mastery experiences • Modeling and vicarious learning • Social persuasion • Physiological and psychological arousal
PsyCap Hope	"[P]ositive motivational state that is based on an interactively derived sense of successful (a) agency (goal directed energy) and (b) pathways (planning to meet goals)" (Snyder et al., 1991, p. 287).	• Goal-setting • Participation • Contingency planning for alternative pathways to attain goals
PsyCap Optimism	Characterizes individuals who "expect things to go their way, and generally believe that good rather than bad things will happen to them." (Scheier et al., 1985).	• Leniency for the past • Appreciation for the present • Opportunity-seeking for the future
PsyCap Resilience	"[T]he positive psychological capacity to rebound, to 'bounce back' from adversity, uncertainty, conflict, failure, or even positive change, progress and increased responsibility" (Luthans, 2002, p. 702)	• Asset-focused strategies such as enhancing employability • Risk-focused strategies such as proactive avoidance of adversity • Process-focused strategies to influence the interpretation of adverse events

Adapted from descriptions in *Psychological capital: Developing the human competitive edge,* Luthans, Youssef, et al. (2007b).

Research Model and Hypotheses

Based on the definition of behavioral complexity, security behavioral complexity entails an insider's security behavioral repertoire and their ability to enact the roles appropriately, termed security differentiation (Hooijberg, 1996; Wu et al., 2010). An insider's security behavioral repertoire is reflected by the roles of protective behaviors identified by Posey et al. (2013) and adapted into a formative construct in this research. Therefore, as described by behavioral complexity, it is hypothesized that security behavioral complexity—composed of security behavioral repertoire and security differentiation—positively impacts an insider's performance of PMBs.

H1: Security Behavioral Repertoire will be positively related to PMBs.

H2: Security Differentiation will be positively related to PMBs.

Effectually performing PMBs requires behavioral complexity as the roles identified in an insider's security behavioral repertoire are often paradoxical and contradictory (Posey et al., 2013). Whether viewing PsyCap as a psychological resource or a positive psychological state, the previously established links between PsyCap and organizational outcomes provide a basis for the relationship between PsyCap and PMBs. For example, PsyCap has been positively linked to an increase in both job performance and satisfaction (Luthans et al., 2007a) as well as increased organizational commitment and citizenship (Avey et al., 2011). The positive impact of job satisfaction, commitment, and citizenship are closely linked and are supported by findings that individuals who are satisfied with their jobs are better organizational citizens and can be expected to perform both in-role and extra-role behaviors to support the organization (Bateman et al., 1983; Williams et al., 1991). Furthermore, PsyCap—by virtue of its association with resilience

and equanimity—is a valuable resource for handling divergent demands or enacting paradoxical roles (Smith et al., 2011). Therefore, PsyCap is hypothesized to be positively related to PMBs (see Figure 4.1).

H3: *PsyCap will be positively related to PMBs.*

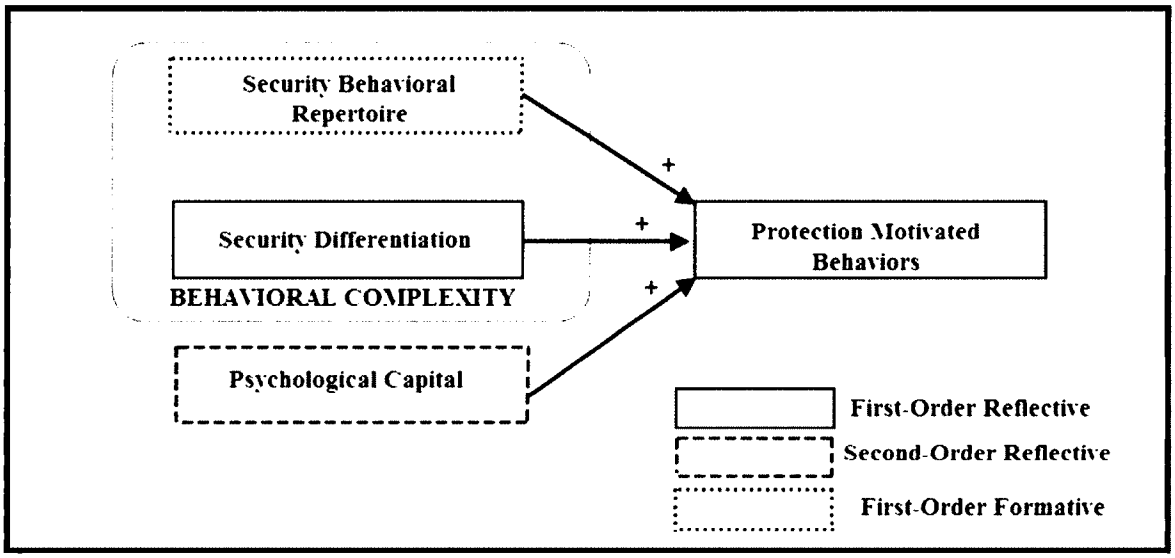


Figure 4.1 Security Behavioral Complexity Research Model

Research Methodology

The multi-dimensional research model was tested empirically using survey research. The instrumentation for the survey was developed based on a thorough literature review. Where possible, the items were adapted from prior research. All the items included in the final survey were subjected to subject matter expert review and pilot tested using a representative sample of organizational insiders from a large public university in the Southeastern United States. The data for the published analyses was collected using an online panel of organizational insiders. Panels are especially appropriate for gathering security data as they offer full anonymity, not simply confidentiality. Given the sensitive nature of security responses, anonymity is required to

encourage candid responses, and panels provide increased anonymity in multiple ways. First, the researchers never know the identity of the respondents, and the privacy of respondents is guaranteed and governed by the data provider. Second, respondents' real and perceived anonymity is enhanced by having access to the survey outside of their organization's network and computers. Providing anonymous, off-site access to self-report surveys has been shown to be adequate and appropriate for the elicitation of self-reported incidences of sensitive and even socially undesirable behaviors such as protection-motivated behaviors (Posey et al., 2013) and organizational deviance (Bennett et al., 2000; Bennett et al., 2003).

Measurement Models

As shown in Figure 4.1, the research model utilizes three distinct latent model structures: first-order reflective constructs, a first-order formative construct, and a second-order reflective construct. Construct specification is a topic of considerable interest in IS research, as the field seeks to employ second generation techniques with both theoretical and statistical validity (Bagozzi, 2011; Gefen et al., 2000; Gefen et al., 2011; Straub et al., 2004; Jarvis et al., 2003). The ultimate goal of all model specification is to appropriately model theoretical relationships; therefore, the on-going discussion regarding the theoretical justification and statistical validity is an important one (Aguirre-Urreta et al., 2012; Jarvis et al., 2012).

The various forms of model specification are "derived from the fact that (a) a first-order construct can have either formative or reflective indicators, and (b) those first-order constructs can, themselves, be either formative or reflective indicators of an underlying second-order construct" (Jarvis et al., 2003). Constructs defined as first- and

second-order reflective appear most often in business research (Jarvis et al., 2003), and specify that the indicators at each level "reflect" the latent variable (Straub et al., 2004; Jarvis et al., 2012). All of the models specified as reflective in the research model were each adapted from prior literature (Luthans et al., 2007b; Wu et al., 2010).

Security behavioral repertoire was developed from the previously developed taxonomy of PMBs (Posey et al., 2013). The developed construct is specified as first-order formative based on Wu et al.'s (2010) repertoire construct and the formative/reflective decision rules provided in prior literature (Jarvis et al., 2003; Petter et al., 2007). Specifically, Wu et al. (2010) measured behavioral repertoire as "the composite of the multiplicative effect of the means of each of the four roles." As noted by Diamantopoulos (2011), modeling a construct with formative specification in partial least squared (PLS) utilizes composites. Therefore, as depicted in Figure 4.1, security behavioral repertoire is specified as formative and will be modeled with PLS as a composite latent variable. This formative specification is in line with previous model specifications in IS (Anderson et al., 2010; Johnston et al., 2010).

Measures in Study

Security behavioral repertoire was measured formatively with items capturing each role of PMBs established in prior research (Posey, 2010). In order to empirically assess the impact of an individual's personal repertoire of security behaviors, I first developed an all-inclusive formative measure of security behavioral repertoires from the published taxonomy of PMBs. The items developed to measure the 14 security roles are shown in Table 4.2. The final construct used in the analysis was refined according to the formative construct specifications in literature.

Table 4.2

Items Developed to Measure 14 Security Roles

Rol	Item
1	I am able to differentiate between legitimate and illegitimate email requests.
2	I can protect my organization's sensitive information that I control from unauthorized exposure.
3	I have the skills to fulfill the requirements of my organization's information security policy.
4	I know how to dispose of the organization's unneeded sensitive documents and backup important documents.
5	I know how to convert sensitive, corporate documents to other formats to reduce potential alterations from their original content by security threats.
6	I am able to use my work-related software (e.g. email clients and Internet browsers) securely.
7	I know what information in my organization is sensitive and should not be disclosed, whether verbally or electronically.
8	I know whether or not I am allowed to set up my own wireless access point at
9	I know how to perform the general security-related tasks required of all employees at work.
10	I know how to perform security-related tasks specific to my position at work.
11	I have the ability to remind my co-workers of information-security guidelines and policies and inform co-workers when they are violating organizational rules.
12	I am able to protect my work-related accounts by safeguarding my log-in
13	I can identify when my co-workers are using IT suspiciously and report it to management.
14	I am able to keep electronic devices (e.g., laptops, tablets, PDAs) issued to me by my organization either safely stored under lock and key or with me at all

Security differentiation was adapted from the five-item measure of behavioral differentiation used in Wu et al. (2010). The measures were adapted from a context of supply management to reflect security differentiation. An example of an item measuring security differentiation is "I adapt my behavior to effectively secure my firm's sensitive information."

PsyCap was measured using the questionnaire developed by Luthans, Youssef et al. (2007b). The PsyCap Questionnaire includes twenty-four items (six for each of the four characteristics). The PsyCap items were all developed from prior literature and have

consistently exhibited validity and test/retest reliability throughout the business literature. (Luthans et al., 2007a; Luthans et al., 2007b).

PsyCap hope measures state-hope and is "responsive to events in the lives of people" (Snyder et al., 1996, p. 321). PsyCap hope captures both the agency and pathway components of hope, and an example of an item measuring PsyCap Hope is "I can think of many ways to reach my current work goals"(Luthans et al., 2007b). *PsyCap Resilience* measures an individual's ability to bounce back or to take stressful things at work in stride (Wagnild et al., 1993). An example of an item measuring resilience is "I usually take stressful things at work in stride" (Luthans et al., 2007b). *PsyCap optimism* measures an individual's state-belief that "good rather than bad things will happen to them" (Scheier et al., 1985, p. 219). An example of an item measuring PsyCap optimism is "I approach this job as if 'every cloud has a silver lining'"(Luthans et al., 2007b). Lastly, *PsyCap self-efficacy* measures the state-like role-breadth self-efficacy and are based on Parker's (1998) self-efficacy scale. An example of an item measuring *PsyCap self-efficacy* is "I feel confident analyzing a long-term problem to find a solution" (Luthans et al., 2007b).

PMBs were measured with a five-item scale developed based on Posey et al.'s (2013) taxonomy of protection-motivated behaviors. An item assessing the performance of PMBs is "I tried to safeguard my organization's information and information systems from their information security threats."

Analysis and Results

The research model was analyzed in a two-step procedure as recommended by methodologists (Gerbing et al., 1988). The analysis utilized partial least squared (PLS)

based structural equation modeling (SEM) platform, SmartPLS (Ringle et al., 2005). In the first step, a confirmatory factor analysis (CFA) was run in order to establish the reliability and validity of the reflective measures to be included in the subsequent structural model. Upon confirmation of the validity of the research model, the hypothesized research model was assessed using SEM. Prior to the collection of the data for the primary analysis, the full instrument was pilot tested.

Pilot Study

Critical to any study is the validity and reliability of the measures employed (Straub, 1989; Gefen et al., 2011). As recommended, whenever possible the scales included in this study were employed as previously published (Straub et al., 2004). The instrument was pilot tested with a sample of 42 MBA students from a large public university in the Southeastern United States. All the students used for the pilot were either currently employed or had previous work experience. The descriptive statistics of the pilot sample are summarized in Table 4.3.

Table 4.3

Descriptive Statistics of Pilot Sample

Average Age		24.26
Average Organizational Tenure		1.66
Gender	Female	31%
	Male	69%
IT Position		4.8%
Management		12.2%

The data from the pilot test was used to examine the validity of the reflective measures to be used in the study. The pilot test construct statistics were ascertained using

partial least squares structural equation modeling (PLS-SEM) in SmartPLS (Ringle et al., 2005). Overall, the results of the pilot test provide evidence of the initial validity of the measures to be used in the full study—the exception being SBD4 which failed to load on the differentiation construct. The construct loadings from the pilot test are summarized in Table 4.4.

Table 4.4

Pilot Study Construct Loadings

	Security Behavioral Differentiation	PMBs	PsyCap
SBD1	0.700		
SBD2	0.851		
SBD3	0.756		
SBD4	0.040		
SBD5	0.746		
PMB1		0.949	
PMB2		0.926	
PMB3		0.946	
PMB4		0.874	
PMB5		0.941	
PCO			0.808
PCSE			0.896
PCH			0.914
PCR			0.925

In addition to viewing the standardized loadings, I also examined the convergent and divergent validity of the constructs by calculating the latent variable correlations, the Cronbach's alpha, and the average variance extracted (AVE) for each of the constructs. The convergent and divergent statistics for the pilot study measures excluding SBD4 are summarized in Table 4.5.

Table 4.5

Pilot Study Correlations

	Security Behavioral Differentiation (SBD)	PMB	PsyCap	Cronbach's α
SBD	**0.83***			0.8971
PMB	0.4279	**0.86**		0.9593
PsyCap	0.4578	0.3871	**0.79**	0.9189
***AVE's** bolded along diagonal				

Primary Study

After analyzing the results of the pilot test and confirming the initial validity of the instrumentation, responses were collected from a sample of 414 organizational insiders. Panels are especially appropriate for gathering security data as they offer full anonymity, not simply confidentiality. Given the sensitive nature of security responses, anonymity is required to encourage candid responses, and panels provide increased anonymity in multiple ways. First, the researchers never know the identity of the respondents, and the privacy of respondents is guaranteed and governed by the data provider. Second, respondents' real and perceived anonymity is enhanced by having access to the survey outside of their organization's network and computers. Providing anonymous, off-site access to self-report surveys has been shown to be adequate and appropriate for the elicitation of self-reported incidences of sensitive and even socially undesirable behaviors such as protection-motivated behaviors (Posey et al., 2013) and organizational deviance (Bennett et al., 2000; Bennett et al., 2003). The descriptive statistics of the primary sample are summarized in Table 4.6.

Table 4.6

Descriptive Statistics of Primary Sample

Average Age		45.59
Average Organizational Tenure		10.58
Gender	Female	53.1%
	Male	46.9%
Education	Some high school	0.2%
	High school diploma	11.4%
	Some college	25.6%
	Undergraduate degree	41.5%
	Master's degree	16.4%
	Doctorate/Professional degree	4.8%
IT Position		15.2%
Management		33.8%

This study employed one formative construct, security behavioral repertoire, which was developed based on a previously published taxonomy of PMBs. In order to assess the validity of security behavioral repertoire, first, the content validly of the items was examined by subject matter experts. Second, the statistical and practical significance of each formative indicator was assessed through the significance and magnitude of the coefficient. Finally, the collinearity of the selected formative items was assessed by calculating the variance inflation factor (VIF) of each indicator from regression analyses.

The validity of the measure of security behavioral repertoire was assessed according to the recommendations for formatively specified constructs (Hair et al., 2014). First, the content validity of the security behavioral repertoire measures was established. Formative measures are modeled to include no measurement error (Bagozzi, 2011); therefore, the formative items are said to fully explain the latent variable. An error in content validity is manifest in the absence of an item which should be included in order to fully represent the construct domain. The formative items measuring security behavioral

repertoire were developed directly from a taxonomy of PMBs (Posey et al., 2013). The taxonomy of PMBs was developed for an identical context (security) and population (organizational insiders). Second, the collinearity of the items was assessed by running regressions of each item on the others in order to ascertain the VIF level of each item. Items with a VIF of greater than ten are said to suffer from multicollinearity, while those with a VIF of five or less are conservatively assessed to have no multicollinearity (D'Arcy et al., 2009; Hair et al., 2014; Hair et al., 2006). The correlations of the 14 roles are shown in Table 4.7.

As expected with such a large number of related, yet distinct roles, the items are correlated with one another with a range of correlation from 0.329 – 0.705. In order to refine the measure of PMB roles, the 14 indicator construct was analyzed using PLS SEM in SmartPLS (Ringle et al., 2005). PLS was chosen for the analysis because of identification issues arising from the inclusion of a formative measure with many indicators.

The initial omnibus security behavioral repertoire construct included 14 security roles and failed to converge using covariance-based SEM. PLS does not share the identification issues with covariance-based SEM. Therefore, analyzing in PLS allows for convergence (Hair et al., 2014). In addition to the PLS analysis, the VIF for each item was calculated by running individual regressions with each item as the dependent variable. The item weights, average VIF, and significance of each role are shown in Table 4.8.

Table 4.7

PMB Roles Correlations

	Role1	Role2	Role3	Role4	Role5	Role6	Role7	Role8	Role9	Role10	Role11	Role12	Role13	Role14
Role1	1													
Role2	.392	1												
Role3	.629	.509	1											
Role4	.666	.329	.633	1										
Role5	.596	.355	.508	.650	1									
Role6	.606	.440	.692	.615	.511	1								
Role7	.588	.507	.697	.565	.526	.703	1							
Role8	.619	.390	.610	.606	.601	.626	.564	1						
Role9	.569	.481	.681	.550	.465	.626	.623	.526	1					
Role10	.477	.401	.502	.496	.545	.430	.494	.437	.450	1				
Role11	.591	.517	.705	.567	.478	.641	.692	.505	.651	.487	1			
Role12	.473	.594	.589	.504	.450	.602	.637	.460	.531	.441	.606	1		
Role13	.410	.629	.533	.338	.375	.528	.528	.432	.578	.366	.512	.532	1	
Role14	.566	.477	.611	.504	.507	.541	.554	.623	.552	.483	.580	.535	.537	1

Table 4.8

PMB Role Statistics

	PMB Role	Avg. VIF	Weight	T-Statistic
1	Legitimate e-mail handling	2.43	0.1862	1.3551
2	Protection against unauthorized exposure	2.44	0.3052	2.3111
3	Policy-driven awareness and action	2.36	-0.0756	1.9078
4	Appropriate data entry and management	2.39	0.2218	1.1169
5	Document conversion	2.43	-0.1066	0.1508
6	Secure software, e-mail, and Internet use	2.38	0.3701	0.4151
7	Verbal and electronic sensitive-information	2.39	0.1872	2.6241
8	Wireless installation	2.42	-0.085	0.5355
9	Widely applicable security etiquette	2.42	0.0822	1.5859
10	Distinctive security etiquette	2.50	0.247	0.8465
11	Co-worker reliance	2.40	-0.2363	2.6375
12	Account protection	2.44	0.1384	1.2446
13	Immediate reporting of suspicious behavior	2.43	-0.0182	0.6164
14	Equipment location and storage	2.44	0.0497	0.609

Many of the 14 roles included initially in the construct of PMB roles failed to exhibit statistical and practical significance. Although none of the VIF statistics surpassed the rule of thumb of five, the high correlations shown in Table 4.7 along with the counter-intuitive weights and lack of significance of many items make it clear that the construct should be subjected to refinement. Therefore, an iterative process of isolating the significant roles making up an insider's security behavioral repertoire was undertaken. I set as an initial decision-rule one-tailed statistical significance of $\alpha = 0.10$ (t-statistic 1.282). This allowed me to retain only those roles which were significantly influencing the construct of security behavioral repertoire while not being overly restrictive in terms of nomological and content validity.

As a result, eight of the 14 roles met the significance criteria for further analyses. The collinearity diagnostics were re-run for these eight roles and they were assessed for adequate domain breadth. The significance of the eight roles along with the collinearity

diagnostics are exhibited in Table 4.8. These roles represent both broad and specific security behaviors (i.e. email use and task specific etiquette), as well as technical and social aspects of security (i.e. secure software use and co-worker reliance). They also include physical as well as intellectual protections (i.e. unauthorized exposure and verbal disclosures) as well as systems protection (i.e. account protection). Therefore, the eight roles are said to meet the criteria for a valid measure of an insider's security behavioral repertoire (see Table 4.9).

Table 4.9

Security Behavioral Repertoire Correlations and T-Statistics

	Role1	Role2	Role4	Role6	Role7	Role10	Role11	Role12	T-Statistic
Legitimate e-mail handling	1								1.441
Protection against unauthorized exposure	.392	1							2.709
Appropriate data entry and management	.666	.329	1						1.546
Secure software, e-mail, and Internet use	.606	.440	.615	1					2.768
Verbal and electronic sensitive-information protection	.588	.507	.565	.703	1				1.468
Distinctive security etiquette	.477	.401	.496	.430	.494	1			2.337
Co-worker reliance	.591	.517	.567	.641	.692	.487	1		1.947
Account protection	.473	.594	.504	.602	.637	.441	.606	1	1.367

For the reflective measures included in the structural model, the standardized factor loadings from a CFA analysis were considered along with the Cronbach's alphas. Also, the convergent and discriminant validity of measures in the structural model were assessed with average variance extracted (AVE) and the Fornell-Larker criterion (i.e., comparison of squared correlations with AVEs) as recommended (Hair et al., 2006; Hair

et al., 2014). The items from the full study and their respective loadings are shown in Table 4.10, followed by the statistics of convergence and discriminance.

Table 4.10

Full Measures in Study

Security Behavioral Repertoire	**Measures**	**Scale[i]**	**Spec.[ii]**	**Mean**	**STD**	**Wt.**
Role1: Legitimate e-mail handling	I am able to differentiate between legitimate and illegitimate email requests.	a	F	5.58	1.45	0.156
Role2: Protection against unauthorized exposure	I can protect my organization's sensitive information that I control from unauthorized exposure.	a	F	4.11	1.80	0.299
Role4: Appropriate data entry and management	I know how to dispose of the organization's unneeded sensitive documents and backup important documents.	a	F	5.70	1.43	0.168
Role6: Secure software, e-mail, and Internet use	I am able to use my work-related software (e.g. email clients and Internet browsers) securely.	a	F	5.22	1.62	0.348
Role7: Verbal and electronic sensitive-information protection	I know what information in my organization is sensitive and should not be disclosed, whether verbally or electronically.	a	F	5.18	1.62	0.168
Role10: Distinctive security etiquette	I know how to perform security-related tasks specific to my position at work.	a	F	5.21	1.72	0.225
Role11: Co-worker reliance	I have the ability to remind my co-workers of information-security guidelines and policies and inform co-workers when they are violating organizational rules.	a	F	5.13	1.68	0.219
Role12: Account protection	I am able to protect my work-related accounts by safeguarding my log-in information.	a	F	4.78	1.72	0.142
Security Differentiation (SBD)	**Adapted from (Wu et al., 2010);**	Scale	Spec.	Mean	STD	Load.
SBD-1	I adapt my behavior to effectively secure my firm's sensitive information.	a	R	5.13	1.486	0.798

Table 4.10 (Continued)

SBD-2	I adjust my approach to my work in order to handle various security threats.	a	R	4.67	1.615	0.862
SBD-3	I take on different security roles at work such as complying with security policy and policing co-workers.	a	R	3.97	1.863	0.864
SBD-4	At work, I may go from screening an illegitimate email request to appropriately discussing my firm's sensitive information with a trusted party.	a	R	3.94	1.870	0.770
SBD-5	When doing different work tasks, I often play different security roles.	a	R	4.01	1.861	0.850
PsyCap Hope (PCH)	**From (Luthans et al., 2007b)**	Scale	Spec.	Mean	STD	Load.
PCH-1	If I should find myself in a jam at work, I could think of many ways to get out of it.	a	R	5.34	1.057	0.757
PCH-2	At the present time, I am energetically pursuing my work goals.	a	R	5.14	1.334	0.768
PCH-4	Right now I see myself as being pretty successful at work.	b	R	5.41	1.054	0.815
PCH-5	I can think of many ways to reach my current work goals.	b	R	5.29	1.246	0.830
PCH-6	At this time, I am meeting the work goals that I set for myself.	b	R	5.45	1.118	0.833
PsyCap Resilience (PCR)	**From (Luthans et al., 2007b)**	Scale	Spec.	Mean	STD	Load.
PCR-2	I usually manage difficulties one way or another at work.	a	R	5.64	.989	0.852
PCR-3	I can be "on my own," so to speak, at work if I have to.	a	R	6.01	1.069	0.780
PCR-4	I usually take stressful things at work in stride.	a	R	5.18	1.202	0.738
PCR-5	I can get through difficult times at work because I've experienced difficulty before.	a	R	5.61	1.069	0.872
PCR-6	I feel I can handle many things at a time at this job.	a	R	5.65	1.111	0.831
PsyCap Optimism (PCO)	**From (Luthans et al., 2007b)**	Scale	Spec.	Mean	STD	Load.
PCO-1	When things are uncertain for me at work, I usually expect the best.	a	R	4.81	1.263	0.834

Table 4.10 (Continued)

PCO-3	I always look on the bright side of things regarding my job.	a	R	5.03	1.521	0.887
PCO-4	I'm optimistic about what will happen to me in the future as it pertains to work.	a	R	5.09	1.277	0.825
PCO-6	I approach this job as if "every cloud has a silver lining."	a	R	4.96	1.421	0.818
PsyCap Self-Efficacy (PCSE)	**From (Luthans et al., 2007b)**	Scale	Spec.	Mean	STD	Load.
PCSE-1	I feel confident analyzing a long-term problem to find a solution.	a	R	5.43	1.143	0.822
PCSE-2	I feel confident in representing my work area in meetings with management.	a	R	5.45	1.274	0.824
PCSE-3	I feel confident contributing to discussions about the company's strategy.	a	R	5.05	1.375	0.805
PCSE-4	I feel confident helping to set targets/goals in my work area.	a	R	5.543	1.250	0.772
PCSE-5	I feel confident contacting people outside the company (e.g., suppliers, customers) to discuss problems.	a	R	5.17	1.482	0.700
PCSE-6	I feel confident presenting information to a group of colleagues.	a	R	5.32	1.347	0.808
Protection Motivated Behaviors (PMB)	**Adapted from (Posey, 2010)**	Scale	Spec.	Mean	STD	Load.
PMB-1	I actively attempted to protect my organization's information and computerized information systems	b	R	4.87	1.900	0.948
PMB-2	I tried to safeguard my organization's information and information systems from their information security threats	b	R	4.94	1.877	0.922
PMB-3	I took committed action to prevent information security threats to my firm's information and computer systems from being successful	b	R	4.52	1.983	0.916

Table 4.10 (Continued)

PMB-4	I purposefully defended my organization from information security threats to its information and computerized information systems	b	R	4.36	1.994	0.880
PMB-5	I earnestly attempted to keep my organization's information and computer systems from harm produced by information security threats	b	R	4.90	1.886	0.938

[i]Scale: a) Strongly Disagree – Strongly Agree
b) Never – Always

[ii]Specification: R) reflective
F) formative

As shown in Table 4.10, a few items were eliminated from the analysis for failing to load significantly on their respective constructs. However, all reflective constructs retained at least four items of which the standardized loadings of the retained reflective items were above a conservative 0.70 cutoff criterion. A loading of 0.70± indicates that the associated latent variable accounts for 50% of the variance in the indicator (Hair et al., 2006; Hair et al., 2014). Supporting the validity of the items, the Cronbach's alpha of each construct was within the recommendations of prior research (Nunnally, 1978), and the constructs exhibited convergence and discriminance as indicated by the AVE and latent variable correlations.

Structural Model

Finally, the hypothesized relationships in the research model were tested using PLS SEM. Unlike covariance-based SEM, PLS analyses do not provide goodness of fit statistics, but rather are assessed by the construct validity and the significance of the

resultant paths (Hair et al., 2014). As can be seen in Tables 4.11 and 4.12, all three of the hypothesized relationships were significant and in the predicted direction.

Table 4.11

Primary Study Correlations

	Security Differentiation (SD)	PMB	PsyCap	Cronbach's α
SD	**0.69***			0.89
PMB	0.4279	**0.85**		0.96
PsyCap	0.4578	0.3871	**0.51**	0.95
*AVE's bolded along diagonal				

Table 4.12

Structural Model Results

Hyp.	Hypothesis (direction)	Path Coefficient	T-value	Significance (one-tailed)
H1	**Security Behavioral Repertoire → PMBs (+)**	**0.33**	**4.914**	***
H2	**Security differentiation→ PMBs (+)**	**0.18**	**2.911**	**
H3	**PsyCap→ PMBs (+)**	**0.14**	**2.931**	**
Controls				
	Age	0.09	2.038	*
	Tenure	-0.04	1.211	n/s
	Gender	0.01	0.052	n/s
	Management	0.03	0.982	n/s
	IT Staff	0.03	1.180	n/s
Bold = supported; *p=0.05; **p=0.01; ***p=0.001; n/s=not significant				

In an effort to establish the robustness of the model of security behavioral complexity, the structural model was also run while controlling for the age, gender, organizational tenure and whether the insider was a member of either management or the

organization's IT staff.[2] In addition, the model was also re-run three additional times including distinct potential rival explanations each time. The security behavioral complexity model was robust to controls for age, gender, and tenure simultaneously, as well as managerial support for security, security locus of control, and social desirability, separately (see Figure 4.2).

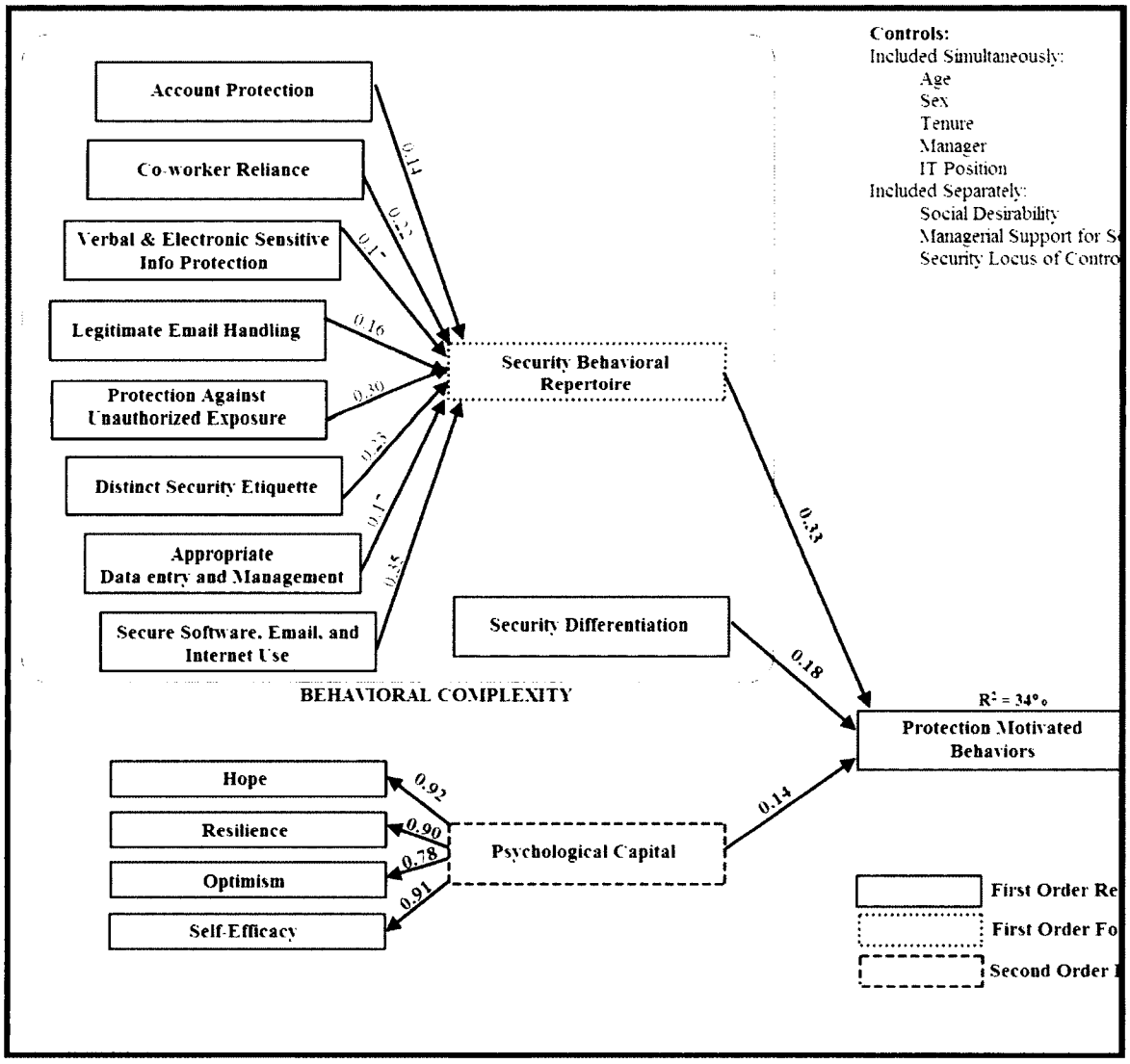


Figure 4.2 *Security Behavioral Complexity Results*

[2] The reduced model including demographic controls is no longer under-identified and was assessed in covariance-based SEM to confirm the results. PsyCap, 0.21, ***; Repertoire, 0.35,***; security differentiation, 0.22,** (construct, path coefficient, significance)

Common Method Variance

All of the indicators in the study were measured by self-report survey items. Although IS research has been shown to be less susceptible to common method variance (CMV) than other disciplines (Malhotra et al., 2006), as a further assessment of the validity of the findings an analysis of CMV was performed. Study design is an important step in avoiding CMV in empirical research (Podsakoff et al., 2003). In order to minimize the effect of CMV in the reported results, several steps were taken in the study design. (1) Respondents were assured of their anonymity by having access to the survey off-site and with a survey organization with which they have a trusted relationship. (2) Within each question set the items were randomly ordered for each respondent, eliminating any systematic bias in the ordering of the items. (3) The question order was counterbalanced with antecedent variables, consequence variables, and control variables dispersed throughout the instrument so as to minimize the likelihood that the responses to independent variables would impact the response to potential dependent variables. The instrument was pilot tested to ensure that the question order did not introduce cognitive labor. (4) The instrument used reverse-order questions as well as "please respond ___" questions in order to identify those respondents who were answering carelessly. (5) Each item was carefully worded to eliminate any biasing effect of item ambiguity.

Given that the analysis was performed using PLS SEM, the methods of detecting and potentially correcting for CMV are more limited than those in covariance-based SEM (Rönkkö et al., 2011). Recently, a marker variable technique has been espoused which can be used to detect methodological bias in PLS (Rönkkö et al., 2011). Despite the efforts to reduce common method bias in the single source data, such a marker variable

was included in the study to allow a post-hoc analyses of CMV. The marker variable included was a construct measuring an individual's feelings about the color blue. An example of an item measuring blue affinity is "I prefer blue to other colors." The responses are a seven point likert scale ranging from "strongly disagree to strongly agree." The use of this variable is more rigorous than using, for example, a demographic response because it is of the same type (i.e. seven-point Likert scale) as the substantive variables in the study (Rönkkö et al., 2011; Williams et al., 2010). The correlation matrix of the substantive, controls, and marker variable are shown in Table 4.13.

The minimum total correlation in the study is 0.00 between differentiation and organizational tenure. However, the minimum correlation between every substantive variable and the marker variable is 0.13. To assess whether or not the relationship between the substantive variables are impacted by a methodological bias, the marker variable was included in the structural model as an antecedent to the single endogenous variable, PMBs. In this way, any variance explained by the theoretically unrelated variable should be associated with methodological bias rather than a true relationship. The marker variable acts as a control of method bias.

Table 4.13

Correlation Matrix Including Marker Variable

	Age	Blue*	Diff	Efficacy	Hope	IT	Mgmt	Optmism	PMBs	PsyCap	Repertoire	Resilience	Gender	Tenure
Age	1													
Blue*	-0.10	1.00												
Differentiation	-0.09	0.14	1.00											
Efficacy	0.07	0.21	0.47	1.00										
Hope	0.06	0.24	0.42	0.76	1.00									
IT	-0.16	-0.02	0.23	0.05	0.05	1.00								
Mgmt.	0.05	-0.08	0.25	0.25	0.19	0.21	1.00							
Optimism	0.02	0.26	0.45	0.59	0.73	0.11	0.16	1.00						
PMBs	0.06	0.13	0.49	0.44	0.38	0.13	0.16	0.35	1.00					
PsyCap	0.07	0.27	0.46	0.91	0.92	0.03	0.20	0.78	0.41	1.00				
Repertoire	-0.02	0.20	0.71	0.54	0.47	0.17	0.16	0.42	0.54	0.54	1.00			
Resilience	0.10	0.26	0.33	0.75	0.77	-0.06	0.12	0.61	0.28	0.90	0.46	1.00		
Gender	0.07	0.01	0.06	0.08	0.02	0.09	0.20	0.05	0.05	0.03	0.06	-0.04	1.00	
Tenure	0.50	-0.04	0.00	0.07	0.08	0.01	0.14	0.03	0.03	0.08	0.04	0.07	0.08	1
*Blue = Marker Variable														

As recommended, the impact to significance and magnitude resulting from the inclusion of the marker variable should be assessed. The changes observed between the baseline model and the marker variable model are shown in Table 4.14. The marker variable failed to significantly explain variance in the endogenous variable (R^2 of both models was 34%). Further, the significance and magnitude of all three substantive variables were unchanged when the marker variable was included in the analysis. These results indicate that method bias is not responsible for the explanation of the dependent variable. Additionally, as discussed, the substantive variables remained significant in the presence of a control for social desirability as well, which further supports a lack of bias in the results.

Table 4.14

Results of Common Method Variance Analysis

Hyp.	Hypothesis (direction)	Path Coefficient	Coefficient Δ	T-value	T-value Δ	Significance Δ
H1	**Security behavioral repertoire→ PMBs (+)**	**0.33**	-	**4.896**	0.018	-
H2	**Security differentiation→ PMBs (+)**	**0.18**	-	**2.882**	0.089	-
H3	**PsyCap→ PMBs (+)**	**0.14**	-	**2.881**	0.050	-
	Controls					
	Age	0.10	.01	2.083	-	-
	Tenure	-0.05	.01	1.215	0.004	-
	Gender	0.00	.01	0.033	0.019	-
	Management	0.03	-	1.027	0.045	-
	IT Staff	0.03	-	1.162	0.018	-
	Marker Variable					
	Blue	0.012	n/a	0.499	n/a	-
*p=0.05; **p=0.01; ***p=0.001; n/a=not applicable						

Discussion

The results of the analysis indicate that the security behavioral security complexity model provides a robust, multidimensional framework of PMB motivation. The three core hypotheses of security behavioral complexity were supported in the analysis and were robust to the inclusion of controls, rival explanations, and a common-method marker construct. As predicted, an individual's security behavioral repertoire is positively related to the performance of PMBs. Security differentiation, or the ability of an insider to differentiate his or her protective behavior according to the situation, was also positively related to the performance of PMBs. Further, as predicted, insiders' PsyCap was positively related to PMBs as well, indicating that PsyCap does provide a necessary resource for taking on the paradoxical roles required by modern information security. Additionally, the varying means and standard deviations of the roles within security behavioral repertoire support the supposition that insider repertoires vary in both breadth and magnitude.

Implications and Contributions

This research makes several important contributions to the behavioral information security literature. First, the study establishes the influence of insiders' security behavioral repertoire on the performance of PMBs. The results underscore the diverse nature of the roles within each insider's security behavioral repertoire as well, with varying means and standard deviations across the roles. The positive relationship between insiders' security behavioral repertoire and PMBs reveals that the broader an insider's repertoire, the greater likelihood that the insider will enact security roles through the performance of PMBs. By capturing security roles through Likert scales, the measures

also capture the magnitude of each role within the insider. Therefore, the results also indicate that the more deeply held the conviction that he or she can enact the roles, the greater the performance of PMBs. Additionally, the formative measure of security behavioral repertoire provides a relative measure of importance of each role in leading to the enactment of the broad category of PMBs.

The influence of security behavioral repertoire provides organizations with evidence of the importance of training the protective security roles individually. Reviewing the formative measurement indicates that certain roles are more strongly related to the performance of PMBs. This realization leads to two conclusions (1) the return to security is unequal across all roles and (2) certain roles do not lead to behavior either because the role is not required or the insider fails to employ a known protection. Therefore, this research provides a measure of effectiveness of the protective roles identified in prior research. Organizations seeking to incite protective behaviors from employees must ensure that the insiders hold the appropriate behaviors within their security behavioral repertoire.

In order to effectively enact the security roles within one's security behavioral repertoire, employees must also be able to switch from one of the roles to another along the course of work. This research provides initial empirical support for this phenomenon which is termed security differentiation. The significance of security differentiation is important for both research and practice. First, insiders who are able to multi-task or change security roles according the dynamic threats encountered in the workplace are more likely to engage in PMBs. This establishes the significance of an important security-related personal characteristic. Organizations seeking to increase security may

seek to train employees to differentiate their behavior or may use this characteristic for screening employees for organizational roles which encounter the most diverse security threats. This significance is summarized in Table 4.15.

Table 4.15

Summary of Key Findings

Finding	**Significance to research**	**Significance to practice**
Varying significance, coefficients, means, and standard deviations of roles included in security behavioral repertoire.	Establishes the uniqueness of each insider's security behavioral repertoire and the relative influence of each role on the performance of PMBs.	Informs organizations as to the uniqueness of each insider's repertoire of security roles and the relative influence of each role on PMBs.
Security behavioral repertoire's positive relationship with PMBs.	Provides evidence that insiders propensity to enact behaviors to protect the firm is directly related to the roles which they hold in their security behavioral repertoire.	Provides support for organizational training of individual security roles in order to increase security by eliciting PMBs from insiders.
Security differentiation's positive relationship with PMBs	Establishes the role of multi-tasking or behavioral diversity on the performance of PMBs and identifies an important security-related characteristic for inclusion into behavioral information security.	Provides organizations with an important characteristic for security-related screening and/or training.
PsyCap's positive relationship with PMBs.	Provides support for the significant role of psychological resources in the enactment of divergent security roles such as PMBs.	Links PsyCap to security, further establishing the positive personal and organizational outcomes attributable to employees' PsyCap.

Finally, beyond the behavioral complexity (repertoire and differentiation), the PsyCap of the insider was a significant antecedent to the performance of PMBs. As

defined previously in the chapter, PsyCap is a set of positive resource capabilities. When dealing with the diverse roles required by modern information security, insiders require psychological resources in order to handle the resulting behavioral tensions. PsyCap provides a measure of these resources and is a significant contributor to the security behavioral complexity research model tested here.

Limitations and Future Research

There are inherent limitations in self-reported security research, and to a large extent this research is no exception. However, due to the absence of observational data of actual security behaviors, survey instruments are an accepted medium for ascertaining the behavior of insiders. I took recommended precaution to ensure that individual anonymity was preserved and responses were uninhibited. Additionally, the data for this research was collected at a cross-sectional level with differences measured between randomly surveyed organizational insiders. As such, this research is an appropriate and important initial validation of the security behavioral complexity model, but research remains to be completed within individuals and at an organizational level.

Eight of the fourteen roles identified as the full taxonomy of PMBs were significantly related to the performance of PMBs. As measured by the security behavioral complexity model, this research examines the relative importance of the roles in insiders' performance of PMBs. Future research remains to examine PMBs at the organizational level in order to ascertain the absolute importance of PMBs in protecting organizations from security threats. Additionally, future research should examine the potential effectiveness of each role in protecting the organization. In that way, organizations will

have a measure of the possible, absolute impact of each role as well as the actual, relative impact of each role.

The impact of differentiation is also an important area for future research. Research remains to establish the ability of organizations to manipulate employee's differentiation. To the extent that differentiation is a malleable characteristic, organizations can increase security by training the diverse enactment of security roles. Additionally, the research supports the notion that employees have varying abilities to differentiate their security behaviors. Future research remains to examine the characteristics of individuals which make them more likely to differentiate their security behaviors. Finally, future research should examine the ability of insiders to differentiate across organizational roles. For example, it may be shown that some departments are more secure due to the self-selection of high differentiators.

Finally, future research should continue to examine the role of positive psychology and positive psychological facets such as those conceptualized in PsyCap in information security. This research adds to the myriad positive outcomes attributable to PsyCap and supports the notion that protective behaviors are impacted positively by positive psychological factors. The security behavioral complexity model is a trainable model, as insiders can have their repertoire expanded and their PsyCap built. Future research should seek to establish effective security programs that capitalize on the malleable qualities of these antecedents to security behaviors in order to maximize the protection of firms' information and information systems.

Conclusion

This dissertation chapter introduced and empirically examined a novel model of security behavioral complexity. The model of security behavioral complexity empirically examines the impact of an insider's security behavioral repertoire, differentiation, and PsyCap on the ultimate performance of PMBs. The results support the model as an appropriate and effective framework of insiders' performance of PMBs. Eight of the fourteen PMB roles were retained in the measure of an insider's security behavioral repertoire and they exhibit the diverse nature of security behaviors in today's connected, techno-centric business and social environments. The retained roles parallel the complex nature of insider's protection of information and IS. The roles are both broad and specific (i.e. email use and task specific etiquette), as well as technical and social (i.e. secure software use and co-worker reliance). They also include physical as well as intellectual protections (i.e. unauthorized exposure and verbal disclosures), as well as systems protection (i.e. account protection).

In addition to merely holding each role within one's behavioral repertoire, the research highlights the inherent role of behavioral diversity in order to enact the various behaviors. This ability is referred to as security differentiation in the chapter and together with security behavioral repertoire makes up behavioral complexity as defined in prior literature. Drawing from the field of positive psychology, this research improves the base model of behavioral complexity by including the psychological resource capabilities of the actor as a significant antecedent to PMBs. The security behavioral complexity model significantly explains over a third of the total variance in the performance of PMBs and is robust to controls and rival explanations.

CHAPTER 5

CONCLUDING CHAPTER

This dissertation and the three studies contained herein empirically examine novel research models in behavioral information security. Central to the research is the relationship between insiders' PsyCap and information security. The findings exhibit the fundamental relationship between information security and PsyCap with support for PsyCap as both an antecedent to security behavior and a consequence of security expectancies. Additionally, the studies incorporate the same dependent variable, performance of protection motivated behaviors (PMBs). The consistency of both PsyCap and PMBs across research models provides a central theme for the investigation of the impact of PsyCap in behavioral information security. PMBs as a dependent variable are of particular importance as they represent behaviors across the domain of protection motivated behaviors which an insider can undertake. The specific results of the three studies are summarized in the remainder of this chapter followed by a recounting of the conclusions drawn from the studies. In addition to summarizing the dissertation findings, the limitations in the dissertation research and opportunities for future research are articulated.

Summary of Dissertation Findings

This concluding chapter next includes a summary of the dissertation findings. The findings of the studies are recapitulated along with a discussion of study-specific limitations and conclusions. Following the specific findings, general conclusions of the dissertation as a whole are detailed.

Study 1: A Multi-Dimensional Assessment of Organizational Insiders' Performance of Protection-Motivated Behaviors: An Expectancy Theory Approach

The first study examined an expectancy-theory based model of insiders' security behavior. Expectancy theory espouses a relationship between valence, instrumentality, and expectancy (VIE) and behavioral motivation. Beyond the relationship between the VIE model and behavioral motivation, the research also examined organizational influence on these dimensions through security education training and awareness (SETA). Finally, the relationship between expectancy dimensions and psychological resources (PsyCap) were also investigated. The motivation to perform protection motivated behaviors (PMBs) was conceptualized as motivation to perform and withdrawal from performance of protective behaviors.

Nine of the thirteen hypothesized relationships were supported in the analysis. The findings support the significant impact of the expectancy dimensions (VIE) on the motivation to and withdrawal from PMBs. As hypothesized, security expectancy and security valence were positively related to protection motivation. Conversely, security valence was negatively related to security withdrawal. In addition the impact of SETA on expectancy dimensions was uniformly supported across the VIE model. Therefore, the security expectancy research model provides a framework for security training for

organizations. Though expectancy theory has been employed at both the within and between individual level in past research, some have argued that expectancy theory is most appropriate for analyzing motivational changes within individuals. However, the robust performance of expectancy between individuals supports its use as a framework of security behavior across individuals. Given the significance of the research model, future research can use this expectancy-based framework to examine within individual impacts resulting from manipulations such as training sessions (see Figure 5.1).

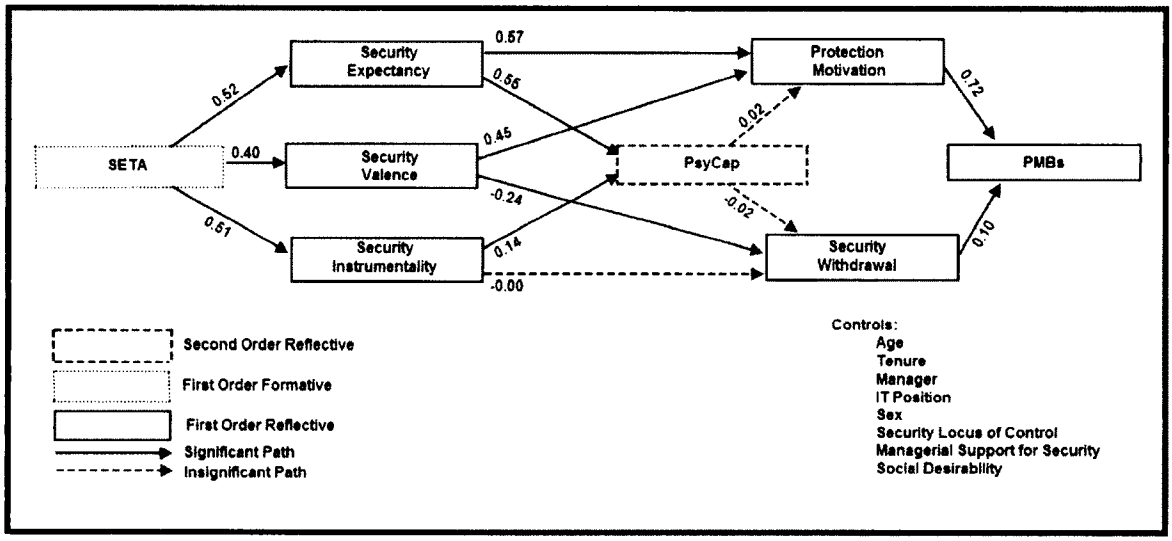


Figure 5.1 *Study One Research Model Summary*

Finally, a significant relationship between the expectancy theory measures of instrumentality and expectancy and PsyCap was established in this research. However, PsyCap was not significantly related to either protection motivation or security withdrawal. Future research should continue to examine the relationship between insiders' PsyCap and security behaviors. Specifically, the role of PsyCap as a resource for security behavior, as a potential moderator of important relationships, and as a dependent variable in IS research should be explored.

Study 2: The Adaptive Role of Emotion in Information Security: Broadening the Theoretical Repertoire

The second study developed and examined a novel model of emotion in behavioral information security. The study offers a complementary emotive-behavioral model to the cognitive-behavioral models which are employed often in IS research. The results of the analysis support the broad influence of emotion in behavioral information security. The research integrates a newly developed framework of emotion with the broaden-and-build theory. Through this integration, the research examines the influence of discrete emotions taking into account the specific action tendencies of each quadrant of the emotional framework (see Figures 5.2 and Figure 5.3).

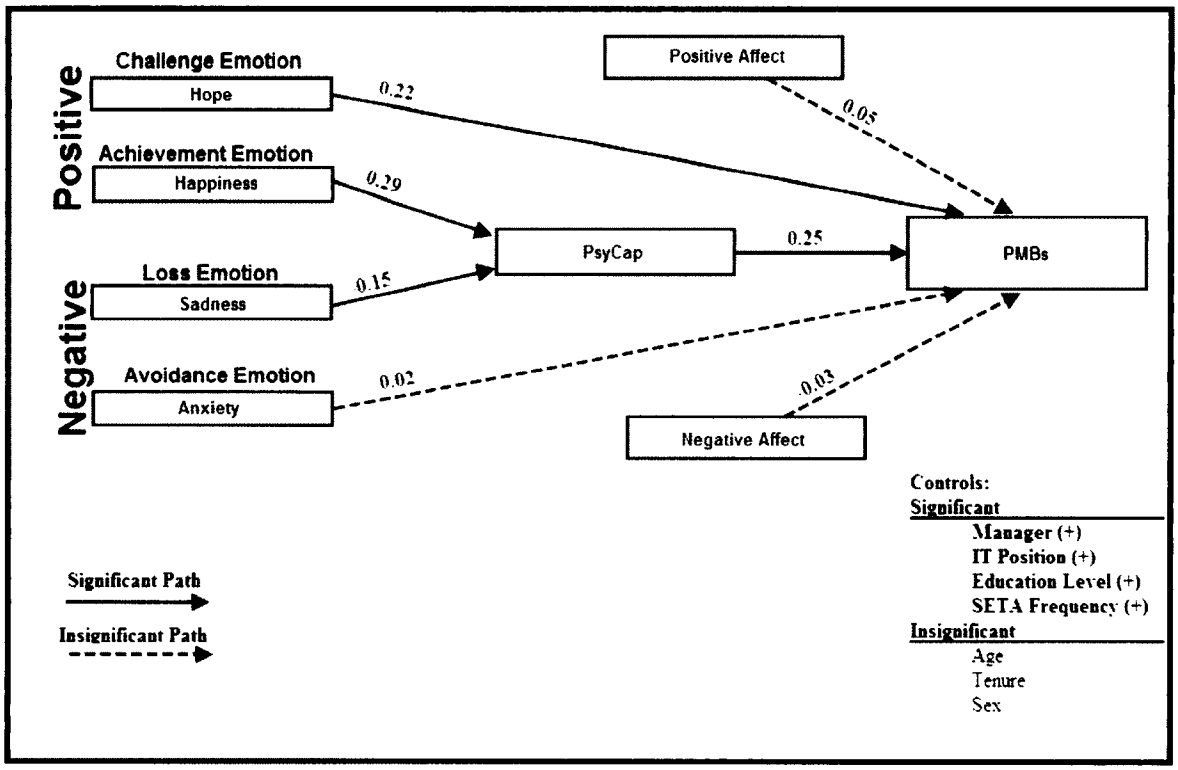


Figure 5.2 *Study Two Research Model 1 Summary*

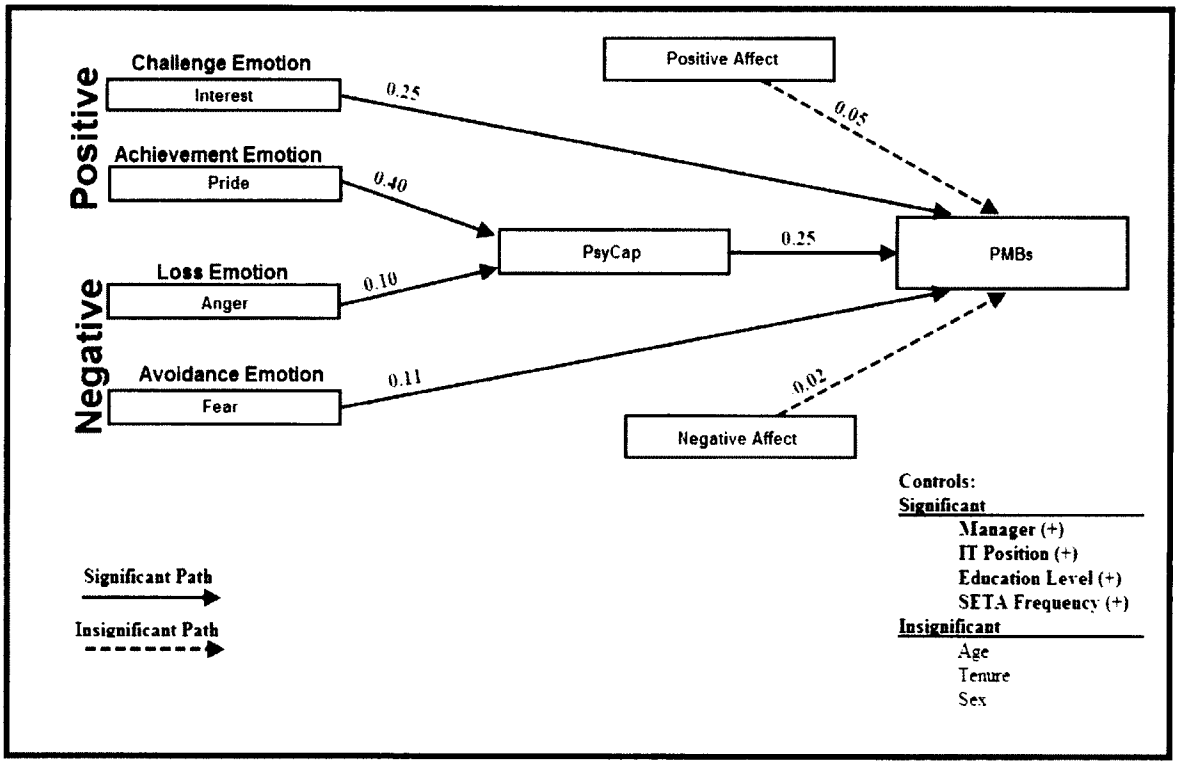


Figure 5.3 *Study Two Research Model 2 Summary*

The discrete emotions were analyzed in two separate models, each with a separate discrete emotion from each quadrant of the emotional framework. The results elucidate the impact of discrete emotions and support the tenants of the broaden-and-build theory. Challenge emotions with their specific action tendency of behavior were positively related to PMBs. Achievement emotions, which are associated with psychological resources, were positively related to PsyCap. On the negative side of the framework, loss emotions were negatively related to PsyCap, and avoidance emotions had mixed results. Anxiety had no relationship with PMBs, while fear was negatively related to PMBs. Lastly, the impact of lingering positive and negative affect were examined in the model and were found to have no impact on PMBs.

Emotional research is not without inherent limitation. The researcher's inability to capture emotional responses from insiders in an experimental setting creates a limitation

in measurement. Due to the difficulty in recalling past emotions, the survey instrument employed in this research asked insiders to respond how they feel when they think about protecting their organization from security threats. Though not experimental, this technique eliminates the temporal disparity between the experience and the survey response.

The emotion-based research model supports the expansion of the theoretical repertoire to include adaptational approaches to security-related behavior such as the broaden-and-build theory, and highlights the need for future research into the impact of positive emotions in behavioral information security and IS at large. Additionally, the research exhibits the importance of research into discrete emotions in behavior information security. As shown in this study, Beaudry and Pinsonneault's (2010) emotional framework provides an important categorization of emotion; however, each discrete emotion retains unique influence as well.

Study 3: Security Behavioral Complexity and Psychological Capital: An Empirical Examination

The third and final study in the dissertation developed and examined a model of security behavioral complexity. Behavioral complexity is comprised of behavioral repertoire and differentiation. The model of security behavioral complexity includes the core components of behavioral complexity, security behavioral repertoire and security differentiation, along with the positive psychological resource of PsyCap.

The findings support the influence of security behavioral complexity on the performance of PMBs by organizational insiders. All three core hypotheses in the model were supported and robust to controls. The results contribute to both research and

practice in several important ways. First the research establishes the influence of behavioral complexity in information security. The impact of security behavioral repertoire on PMBs supports the notion that insiders' performance of PMBs is related to the security behavioral repertoire of insiders. The relationship between security behavioral repertoire and PMBs provides organizations with a framework for developing training programs (SETA). The positive influence of differentiation evidences the importance of behavioral diversity in modern information security. Finally, the influence of PsyCap indicates that in light of behavioral complexity, psychological resources are influential in behavior as well (see Figure 5.4).

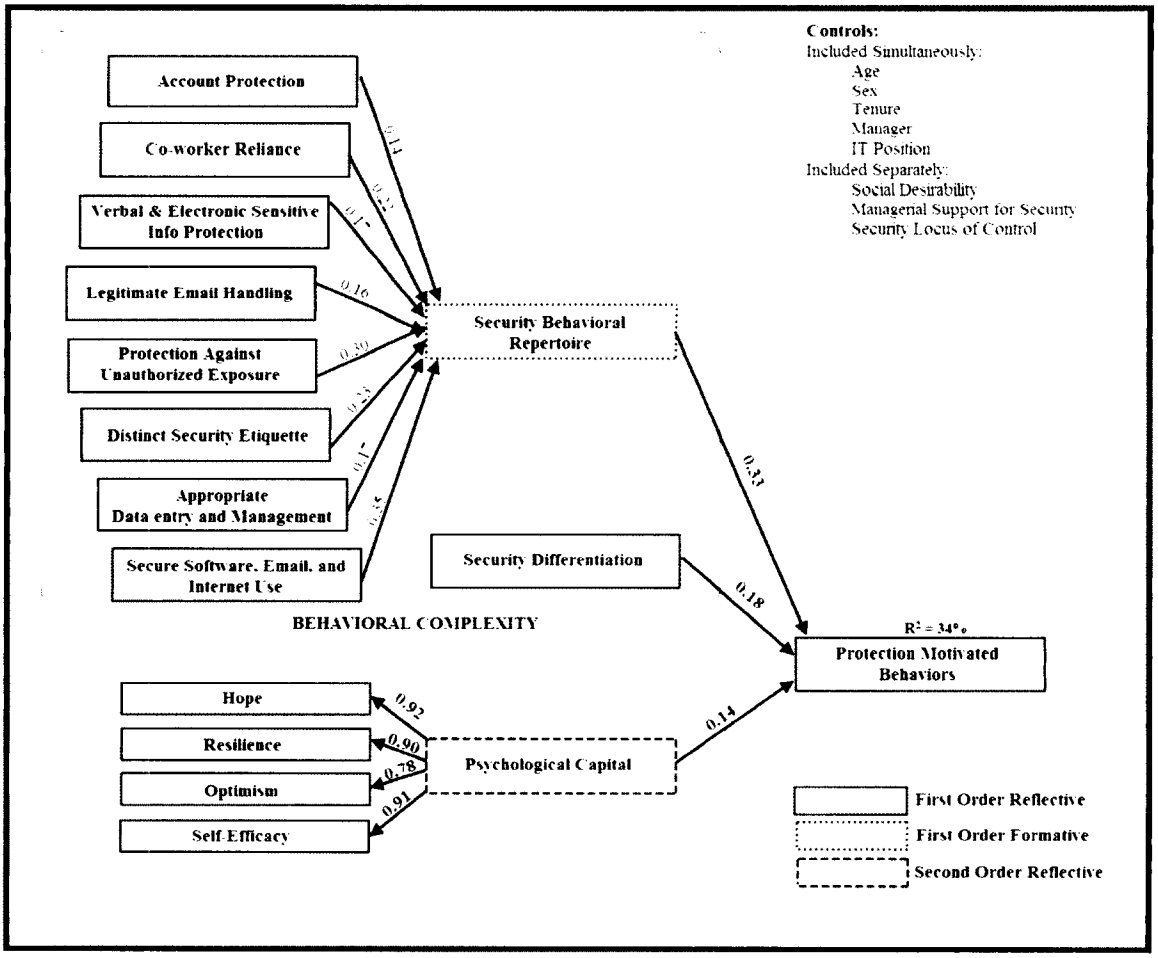


Figure 5.4 *Study Three Research Model Summary*

The results of the security behavioral complexity research present opportunities for future research. For example, future research remains to establish the potential effectiveness of each role which an insider may hold in his or her security behavioral repertoire. The influence of security differentiation also presents an area for future research. Researcher into the malleability of security differentiation would establish the most appropriate mechanism by which to increase security in light of the impact of differentiation, whether through training differentiation or screening for levels of differentiation.

Dissertation Limitations

There are inherent limitations in self-reported security research, and to a large extent this research is no exception. However, due to the absence of observational data of actual security behaviors, survey instruments are an accepted medium for ascertaining the behavior of insiders. I took recommended precaution to ensure that individual anonymity was preserved and responses were uninhibited. Additionally, the data for this research was collected at a cross-sectional level using an online panel with differences measured between randomly surveyed organizational insiders.

Panels are especially appropriate for gathering security data as they offer full anonymity, not simply confidentiality. Given the sensitive nature of security responses, anonymity is required to encourage candid responses, and panels provide increased anonymity in multiple ways. First, the researchers never know the identity of the respondents, and the privacy of respondents is guaranteed and governed by the data provider. Second, respondents' real and perceived anonymity is enhanced by having access to the survey outside of their organization's network and computers. Providing

anonymous, off-site access to self-report surveys has been shown to be adequate and appropriate for the elicitation of self-reported incidences of sensitive and even socially undesirable behaviors such as protection-motivated behaviors (Posey et al., 2013) and organizational deviance (Bennett et al., 2000; Bennett et al., 2003). Finally, all instruments were pilot tested before execution. As such, the dissertation results were based on the surveying of four unique samples—two pilot study samples and two large online panels.

Final Conclusions and Future Research

The dissertation examined the role of PsyCap in behavioral security. The role of PsyCap as an important consequence of and antecedent to security-related constructs was established in the work. The dissertation sets the stage for significant future research in behavioral information security. First, future research into the relationship between PsyCap and information security should be researched further. The studies reveal PsyCap to be a significant antecedent and consequence of security-related constructs. The role of PsyCap in information security highlights the importance of psychological resources in the protection of the firm's informational assets. In this hyper-connected organizational environment, the psychological resources of all those with access to proprietary information is likely to be an important future consideration. Additionally, the almost daily reportage of insider misbehavior support future research into the role that positive psychological resources may play in the commission of deviant behaviors as well.

The dissertation also provides support for the investigation into PMBs. All three dissertation studies explore theoretical frameworks for the explanation of performance of PMBs. As a construct reflecting a general class of protective behaviors, research into

PMBs allows for consideration across the full domain of protective behaviors simultaneously. Future research remains to be conducted into the performance of PMBs. PMBs are an important future dependent variable as they represent the full domain of protective behaviors which an insider can hold in his or her security behavioral repertoire. Therefore, they allow for the investigation into a class of behaviors rather than relegation to specific behaviors.

REFERENCES

Abbas, M., Raja, U., Darr, W., and Bouckenooghe, D. 2012. "Combined Effects of Perceived Politics and Psychological Capital on Job Satisfaction, Turnover Intentions, and Performance," *Journal of Management*.

Abraham, C., Boudreau, M. C., Junglas, I., and Watson, R. 2013. "Enriching our theoretical repertoire: the role of evolutionary psychology in technology acceptance," *European Journal of Information Systems* (22), pp 56-75.

Abramson, L. Y., Seligman, M. E., and Teasdale, J. D. 1978. "Learned helplessness in humans: Critique and reformulation," *Journal of abnormal psychology* (87:1), p 49.

Aguirre-Urreta, M. I., and Marakas, G. M. 2012. "Revisiting bias due to construct misspecification: different results from considering coefficients in standardized form," *MIS Quarterly* (36:1), pp 123-138.

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp 179-211.

Ajzen, I., and Fishbein, M. 1972. "Attitudes and normative beliefs as factors influencing behavioral intentions," *Journal of Personality and Social Psychology* (21:1), p 1.

Albrechtsen, E., and Hovden, J. 2009. "The information security digital divide between information security managers and users," *Computers & Security* (28:6), pp 476-490.

Allen, B. P., and Potkay, C. R. 1981. "On the arbitrary distinction between states and traits," *Journal of personality and social psychology* (41:5), p 916.

Amabile, T. M., Barsade, S. G., Mueller, J. S., and Staw, B. M. 2005. "Affect and creativity at work," *Administrative Science Quarterly* (50:3), p 367.

Anderson, C. L., and Agarwal, R. 2010. "Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions," *MIS quarterly* (34:3), pp 613-643.

August, T., and Tunca, T. I. 2006. "Network software security and user incentives," *Management Science* (52:11), pp 1703-1720.

Avey, J. B., Luthans, F., and Jensen, S. M. 2009. "Psychological capital: A positive resource for combating employee stress and turnover," *Human Resource Management* (48:5), pp 677-693.

Avey, J. B., Luthans, F., Smith, R. M., and Palmer, N. F. 2010. "Impact of positive psychological capital on employee well-being over time," *Journal of Occupational Health Psychology* (15:1), p 17.

Avey, J. B., Patera, J. L., and West, B. J. 2006. "The implications of positive psychological capital on employee absenteeism," *Journal of Leadership & Organizational Studies* (13:2), pp 42-60.

Avey, J. B., Reichard, R. J., Luthans, F., and Mhatre, K. H. 2011. "Meta analysis of the impact of positive psychological capital on employee attitudes, behaviors, and performance," *Human Resource Development Quarterly* (22:2), pp 127-152.

Ayyagari, R., Grover, V., and Purvis, R. 2011. "Technostress: technological antecedents and implications," *MIS Quarterly* (35:4), pp 831-858.

Bagozzi, R. P. 2011. "Measurement and meaning in information systems and organizational research: methodological and philosophical foundations," *MIS Quarterly* (35:2), pp 261-292.

Bagozzi, R. P., Gopinath, M., and Nyer, P. U. 1999. "The role of emotions in marketing," *Journal of the Academy of Marketing Science* (27:2), p 184.

Bandura, A. 1977. "Self-efficacy: toward a unifying theory of behavioral change," *Psychological review* (84:2), p 191.

Barrett, F. J. 1998. "Coda—Creativity and Improvisation in Jazz and Organizations: Implications for Organizational Learning," *Organization Science* (9:5), pp 605-622.

Bateman, T. S., and Organ, D. W. 1983. "Job Satisfaction and the Good Soldier: The Relationship Between Affect and Employee" Citizenship"," *Academy of management journal* (26:4), pp 587-595.

Beaudry, A., and Pinsonneault, A. 2010. "The other side of acceptance: studying the direct and indirect effects of emotions on information technology use," *MIS Quarterly* (34:4), pp 689-710.

Beer, G. 1980. "The Cobb-Douglas Production Function," *Mathematics Magazine* (53:1), pp 44-48.

Bennett, R. J., and Robinson, S. L. 2000. "Development of a measure of workplace deviance," *The Journal of applied psychology* (85:3), pp 349-360.

Bennett, R. J., and Robinson, S. L. 2003. The past, present, and future of workplace deviance research. In J. Greenberg (Ed.), *Organizational Behavior: The state of the science* (2nd edn, pp. 247-281). Mahwah, NJ: Erlbaum.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *European Journal of Information Systems* (18:2), pp 151-164.

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., and Buckalew, L. 2012. "BYOD: A global perspective."

Brouer, R. L., Harris, K. J., and Kacmar, K. M. 2011. "The moderating effects of political skill on the perceived politics–outcome relationships," *Journal of Organizational Behavior* (32:6), pp 869-885.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (221:243), p 243.

Burton, F. G., Chen, Y.-N., Grover, V., and Stewart, K. A. 1992. "An application of expectancy theory for assessing user motivation to utilize an expert system," *Journal of Management Information Systems*, 9(3), pp 183-198.

Cacioppo, J. T., Gardner, W. L., and Berntson, G. G. 1999. "The affect system has parallel and integrative processing components: Form follows function," *Journal of Personality and Social Psychology* (76:5), p 839.

Capra, C. M., and Rubin, P. H. 2011. "Rationality and utility: economics and evolutionary psychology," In *Evolutionary Psychology in the Business Sciences* (pp. 319-338). Springer Berlin Heidelberg.

Carver, C. S., and Scheier, M. F. 1982. "Control theory: A useful conceptual framework for personality–social, clinical, and health psychology," *Psychological bulletin* (92:1), p 111.

Carver, C. S., and Scheier, M. F. 1990. "Origins and functions of positive and negative affect: A control-process view," *Psychological review* (97:1), p 19.

CDW, I. 2013. "CDW Canada survey reveals mobility and bring-your-own-device a top technology priority for Canadian businesses this year," in *The Scaramento Bee*: Sacramento, California.

Cenfetelli, R. T. 2004. "Getting in touch with our feelings towards technology," Academy of Management Annual Conference.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of information security in the workplace: linking information security climate to compliant behavior," *Journal of information privacy and security* (1:3), pp 18-41.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. 2007. "Management of Information Security: Challenges and Research Directions," *Communications of AIS* (20:20), pp 958-971.

Cosmides, L., and Tooby, J. 2000. "Evolutionary psychology and the emotions," *Handbook of emotions* (2), pp 91-115.

Courtney, J. F., DeSanctis, G., and Kasper, G. M. 1983. "Continuity in MIS/DSS Laboratory Research: The Case For A Common Game Simulator," *Decision Sciences* (14:3), pp 419-439.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2012. "Future Directions for Behavioral Information Security Research," *Computers & Security*.

Culbertson, S. S., Fullagar, C. J., and Mills, M. J. 2010. "Feeling good and doing great: The relationship between psychological capital and well-being," *Journal of Occupational Health Psychology* (15:4), p 421.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences (*43:6), pp 1091-1124..

D'Arcy, J., and Herath, T. 2011. "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings," *European journal of information systems* (20:6), pp 643-658.

D'Arcy, J., and Hovav, A. 2007. "Deterring internal information systems misuse," *Communications of the ACM* (50:10), pp 113-117.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information systems research* (20:1), pp 79-98.

Davis, F. D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly* (13:3), pp 319-340.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1992. "Extrinsic and intrinsic motivation to use computers in the workplace1," *Journal of Applied Social Psychology* (22:14), pp 1111-1132.

Denison, D. R., Hooijberg, R., and Quinn, R. E. 1995. "Paradox and performance: Toward a theory of behavioral complexity in managerial leadership," *Organization Science* (6:5), pp 524-540.

DeSanctis, G. 1983. "Expectancy theory as an explanation of voluntary use of a decision-support system," *Psychological Reports* (52:1), pp 247-260.

DeSteno, D., Petty, R. E., Rucker, D. D., Wegener, D. T., and Braverman, J. 2004. "Discrete emotions and persuasion: the role of emotion-induced expectancies," *Journal of Personality and Social Psychology; Journal of Personality and Social Psychology* (86:1), p 43.

Dhillon, G., and Backhouse, J. 2001. "Current directions in IS security research: towards socio-organizational perspectives," *Information Systems Journal* (11:2), pp 127-153.

Dhillon, G., and Torkzadeh, G. 2006. "Value-focused assessment of information system security in organizations," *Information Systems Journal* (16:3), pp 293-314.

Diamantopoulos, A. 2011. "Incorporating formative measures into covariance-based structural equation models," *MIS Quarterly* (35:2), pp 335-358.

Diener, C. I., and Dweck, C. S. 1980. "An analysis of learned helplessness: II. The processing of success," *Journal of personality and social psychology* (39:5), p 940.

Diener, E., and Emmons, R. A. 1984. "The independence of positive and negative affect," *Journal of personality and social psychology* (47:5), p 1105.

Drucker, P. F. 2011. *The new realities*, New York, NY: Routledge .

Dweck, C. S. 1975. "The role of expectations and attributions in the alleviation of learned helplessness," *Journal of personality and social psychology* (31:4), p 674.

Egloff, B., Schmukle, S. C., Burns, L. R., Kohlmann, C. W., and Hock, M. 2003. "Facets of dynamic positive affect: differentiating joy, interest, and activation in the positive and negative affect schedule (PANAS)," *Journal of Personality and Social Psychology* (85:3), p 528.

Ellingson, J. E., and McFarland, L. A. 2011. "Understanding faking behavior through the lens of motivation: An application of VIE theory," *Human Performance* (24:4), pp 322-337.

Feather, N. T. 1969. "Attribution of responsibility and valence of success and failure in relation to initial confidence and task performance," *Journal of Personality and Social Psychology* (13:2), p 129.

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., and Gruen, R. J. 1986. "Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes," *Journal of Personality and Social Psychology; Journal of Personality and Social Psychology* (50:5), p 992.

Forgas, J. P., and George, J. M. 2001. "Affective influences on judgments and behavior in organizations: An information processing perspective," *Organizational behavior and human decision processes* (86:1), pp 3-34.

Fredrickson, B. L. 1998. "What good are positive emotions?," *Review of general psychology* (2:3), p 300.

Fredrickson, B. L. 2001. "The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions," *American psychologist* (56:3), p 218.

Fredrickson, B. L. 2004. "The broaden-and-build theory of positive emotions," *Philosophical Transactions - Royal Society of London Series B Biological Sciences*, pp 1367-1378.

Fredrickson, B. L., and Branigan, C. 2005. "Positive emotions broaden the scope of attention and thought-action repertoires," *Cognition & Emotion* (19:3), pp 313-332.

Fredrickson, B. L., and Cohn, M. A. 2008. "Positive emotions," *Handbook of emotions* (3), pp 777-796.

Fredrickson, B. L., and Joiner, T. 2002. "Positive emotions trigger upward spirals toward emotional well-being," *Psychological science* (13:2), pp 172-175.

Fredrickson, B. L., Tugade, M. M., Waugh, C. E., and Larkin, G. R. 2003. "What good are positive emotions in crises? A prospective study of resilience and emotions following the terrorist attacks on the United States on September 11th, 2001," *Journal of personality and Social Psychology* (84:2), p 365.

Frijda, N. H. 1988. "The laws of emotion," *American psychologist* (43:5), p 349.

Fudge, R. S., and Schlacter, J. L. 1999. "Motivating employees to act ethically: An expectancy theory approach," *Journal of Business Ethics* (18:3), pp 295-304.

Fugate, M., Prussia, G. E., and Kinicki, A. J. 2012. "Managing Employee Withdrawal During Organizational Change The Role of Threat Appraisal," *Journal of Management* (38:3), pp 890-914.

Gable, S. L., and Haidt, J. 2005. "What (and why) is positive psychology?," *Review of general psychology* (9:2), p 103.

Galbraith, J., and Cummings, L. L. 1967. "An empirical investigation of the motivational determinants of task performance: Interactive effects between instrumentality—valence and motivation—ability," *Organizational behavior and human performance* (2:3), pp 237-257.

Gefen, D., Straub, D. W., and Boudreau, M. C. 2000. "Structural equation modeling and regression: Guidelines for research practice," *Communications of the Association for Information Systems* (4).

Gefen, D., Straub, D. W., and Rigdon, E. E. 2011. "An Update and Extension to SEM Guidelines for Admnistrative and Social Science Research," *Management Information Systems Quarterly* (35:2), pp iii-xiv.

Gerbing, D. W., and Anderson, J. C. 1988. "An updated paradigm for scale development incorporating unidimensionality and its assessment," *Journal of marketing research* (25:2), pp 186-192.

Gimeno, J., Folta, T. B., Cooper, A. C., and Woo, C. Y. 1997. "Survival of the fittest? Entrepreneurial human capital and the persistence of underperforming firms," *Administrative science quarterly* (42:4), pp 750-783.

Goldberg, L. R. 1990. "An alternative" description of personality": The Big-Five factor structure," *Journal of personality and social psychology* (59:6), p 1216.

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., and Hull, T. D. 2008. "Combating the insider cyber threat," *Security & Privacy, IEEE* (6:1), pp 61-64.

Griskevicius, V., Ackerman, J. M., Bergh, B., and Li, Y. J. 2011. "Fundamental Motives and Business Decisions," In *Evolutionary Psychology in the Business Sciences* (pp. 17-40). Springer Berlin Heidelberg.

Hair, J., Black, W., Babin, B., Anderson, R., and Tatham, R. 2006. "Multivariate Data Analysis (6^{th} ed.). Upper Saddle River, NJ: Pearson Education.

Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2014. *A Primer on Partial Least Squares Structural Equations Modeling (PLS-SEM)*, SAGE Publications.

Hamill, J. T., Deckro, R. F., and Kloeber, J. M. 2005. "Evaluating information assurance strategies," *Decision Support Systems* (39:3), pp 463-484.

Hantula, D. A., Kock, N., D'Arcy, J. P., and DeRosa, D. M. 2011. "Media Compensation Theory: A Darwinian Perspective on Adaptation to Electronic Communication and Collaboration," In *Evolutionary Psychology in the Business Sciences* (pp. 339-363). Springer Berlin Heidelberg.

Herath, T., and Rao, H. R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp 106-125.

Hobfoll, S. E. 1989. "Conservation of resources: A new attempt at conceptualizing stress," *American psychologist* (44:3), p 513.

Hobfoll, S. E. 2002. "Social and psychological resources and adaptation," *Review of general psychology* (6:4), p 307.

Hom, P. W., Mitchell, T. R., Lee, T. W., and Griffeth, R. W. 2012. "Reviewing employee turnover: Focusing on proximal withdrawal states and an expanded criterion," *Psychological bulletin* (138:5), p 831.

Hooijberg, R. 1996. "A multidirectional approach toward leadership: An extension of the concept of behavioral complexity," *Human Relations* (49:7), pp 917-946.

Hu, L., and Bentler, P. M. 1999. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Structural Equation Modeling: A Multidisciplinary Journal* (6:1), pp 1-55.

Huettner, D. A., and Costanza, R. 1982. "Economic values and embodied energy," *Science* (216:4550), pp 1141-1143.

Hulin, C. L., Roznowski, M., and Hachiya, D. 1985. "Alternative opportunities and withdrawal decisions: Empirical and theoretical discrepancies and an integration," *Psychological bulletin* (97:2), p 233.

Ilgen, D. R., Nebeker, D. M., and Pritchard, R. D. 1981. "Expectancy theory measures: An empirical comparison in an experimental simulation," *Organizational Behavior and Human Performance* (28:2), pp 189-223.

Im, G. P., and Baskerville, R. L. 2005. "A longitudinal study of information system threat categories: the enduring problem of human error," *ACM SIGMIS Database* (36:4), pp 68-79.

Isen, A. M. 1999. "Positive affect," *Handbook of cognition and emotion*), pp 521-539.

Izard, C. E. 1977. *Human emotions*, New York, NY: Plenum Press.

James, W. 1884. "II.—What is an Emotion?" *Mind* (34), p 188.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2003. "A critical review of construct indicators and measurement model misspecification in marketing and consumer research," *Journal of Consumer Research* (30:2), pp 199-218.

Jarvis, C. B., MacKenzie, S. B., and Podsakoff, P. M. 2012. "The negative consequences of measurement model misspecification: a response to Aguirre-Urreta and Marakas," *MIS Quarterly* (36:1), pp 139-146.

Johnson, M. E. 2008. "Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain," *Journal of Management Information Systems* (25:2), pp 97-124.

Johnson, M. E., Goetz, E., and Pfleeger, S. L. 2009. "Security through information risk management," *IEEE Security and Privacy* (7:3), pp 45-52.

Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: an empirical study," *MIS Quarterly* (34:3), pp 549-566.

Judge, T. A., and Bono, J. E. 2001. "Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis," *Journal of Applied Psychology* (86:1), p 80.

Kaplan, S., Bradley, J. C., Luchman, J. N., and Haynes, D. 2009. "On the role of positive and negative affectivity in job performance: a meta-analytic investigation," *Journal of Applied Psychology* (94:1), p 162.

Keaveney, S. M., and Nelson, J. E. 1993. "Coping with organizational role stress: Intrinsic motivational orientation, perceived role benefits, and psychological withdrawal," *Journal of the Academy of Marketing Science* (21:2), pp 113-124.

Kiesler, S., and Sproull, L. 1982. "Managerial response to changing environments: Perspectives on problem sensing from social cognition," *Administrative Science Quarterly* (27:4), pp 548-570.

Kline, R. B. 2010. *Principles and practice of structural equation modeling*. New York, NY: Guilford press.

Kock, N. 2009. "Information systems theorizing based on evolutionary psychology: an interdisciplinary review and theory integration framework," *MIS Quarterly* (33:2), pp 395-418.

Kumar, R. L., Park, S., and Subramaniam, C. 2008. "Understanding the value of countermeasure portfolios in information systems security," *Journal of Management Information Systems* (25:2), pp 241-280.

Lazarus, R. S. 1991. *Emotion and adaptation*. New York, NY: Oxford University Press.

Lazarus, R. S., and Folkman, S. 1984. *Stress, appraisal, and coping*. New York, NY: Springer Publishing Company.

Leach, J. 2003. "Improving user security behaviour," *Computers & Security* (22:8), pp 685-692.

Lee, J., and Lee, Y. 2002. "A holistic model of computer abuse within organizations," *Information Management & Computer Security* (10:2), pp 57-63.

Lee, Y., and Larsen, K. R. 2009. "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software," *European Journal of Information Systems* (18:2), pp 177-187.

Luthans, F. 2002. "The need for and meaning of positive organizational behavior," *Journal of Organizational Behavior* (23:6), pp 695-706.

Luthans, F., Avey, J. B., Avolio, B. J., Norman, S. M., and Combs, G. M. 2006a. "Psychological capital development: toward a micro intervention," *Journal of Organizational Behavior* (27:3), pp 387-393.

Luthans, F., Avey, J. B., Avolio, B. J., and Peterson, S. J. 2010. "The development and resulting performance impact of positive psychological capital," *Human Resource Development Quarterly* (21:1), pp 41-67.

Luthans, F., and Avolio, B. J. 2009. "The "point" of positive organizational behavior," *Journal of Organizational Behavior* (30:2), pp 291-307.

Luthans, F., Avolio, B. J., Avey, J. B., and Norman, S. M. 2007a. "Positive psychological capital: Measurement and relationship with performance and satisfaction," *Personnel Psychology* (60:3), pp 541-572.

Luthans, F., Norman, S. M., Avolio, B. J., and Avey, J. B. 2008. "The mediating role of psychological capital in the supportive organizational climate—employee performance relationship," *Journal of Organizational Behavior* (29:2), pp 219-238.

Luthans, F., Vogelgesang, G. R., and Lester, P. B. 2006b. "Developing the psychological capital of resiliency," *Human Resource Development Review* (5:1), pp 25-44.

Luthans, F., Youssef, C. M., and Avolio, B. J. 2007b. *Psychological capital: Developing the human competitive edge.* New York, NY: Oxford University Press.

Mackinnon, A., Jorm, A. F., Christensen, H., Korten, A. E., Jacomb, P. A., and Rodgers, B. 1999. "A short form of the Positive and Negative Affect Schedule: Evaluation of factorial validity and invariance across demographic variables in a community sample," *Personality and Individual differences* (27:3), pp 405-416.

Maier, S. F., and Seligman, M. E. 1976. "Learned helplessness: Theory and evidence," *Journal of Experimental Psychology: General; Journal of Experimental Psychology: General* (105:1), p 3.

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research," *Management Science* (52:12), pp 1865-1883.

Masten, A. S. 2001. "Ordinary magic: Resilience processes in development," *American Psychologist* (56:3), p 227.

Masten, A. S., and Reed, M. G. J. 2002. "Resilience in development," In C.R. Snyder and S.J. Lopez (Eds.), *Handbook of positive psychology*, (pp 74-88). New York, NY: Oxford University Press.

Moore, A. P., Cappelli, D. M., and Trzeciak, R. F. 2008. "The "big picture" of insider it sabotage across us critical infrastructures," *Insider Attack and Cyber Security*, pp 17-52.

Muthén, L., and Muthén, B. 1998-2010. "Mplus User's Guide," Muthén & Muthén: Los Angeles, CA.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems* (18:2), pp 126-139.

Nabi, R. 2002. "Anger, fear, uncertainty, and attitudes: A test of the cognitive-functional model," *Communication Monographs* (69:3), pp 204-216.

Nesse, R. M., and Ellsworth, P. C. 2009. "Evolution, emotions, and emotional disorders," *American psychologist* (64:2), p 129.

Nunnally, J. 1978. *Psychometric theory*. New York, NY: McGraw-Hill.

Öhman, A., and Mineka, S. 2001. "Fears, phobias, and preparedness: toward an evolved module of fear and fear learning," *Psychological review* (108:3), p 483.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' behavior towards IS security policy compliance," Proceedings of the 40th Annual Hawaii International Conference on Information Systems (HICSS).

Parker, S. K. 1998. "Enhancing role breadth self-efficacy: the roles of job enrichment and other organizational interventions," *The Journal of applied psychology* (83:6), pp 835-852.

Peterson, S. 2012. "Leaders, Cheer Up! Positive Thinking can Boost Organizational Performance," in *KnowMgmt*, W. P. Carey School of Business.

Peterson, S., Luthans, F., Avolio, B. J., Walumbwa, F. O., and Zhang, Z. 2011. "Psychological capital and employee performance: A latent growth modeling approach," *Personnel Psychology* (64:2), pp 427-450.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying formative constructs in information systems research," *Management Information Systems Quarterly* (31:4), p 623.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., and Podsakoff, N. P. 2003. "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *Journal of Applied Psychology* (88:5), p 879.

Ponemon 2013. "The Risk of Insider Fraud - Second Annual Study," Ponemon Institute, LLC.

Posey, C. 2010. *Protection-motivated behaviors of organizational insiders,* Dissertation, Louisiana Tech University, Ruston, Louisiana.

Posey, C., Bennett, B., Roberts, T., and Lowry, P. 2011. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security* (7:1), pp 24-47.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly.*

Richardson, R. 2010/2011. "CSI computer crime and security survey," *Computer Security Institute (GoCSI.com)*, pp 1-42.

Ringle, C. M., Wende, S., and Will, A. 2005. "SmartPLS, release 2.0 (beta)," *SmartPLS, Hamburg, Germany. URL http://www. smartpls. de.*

Rönkkö, M., and Ylitalo, J. 2011. "PLS marker variable approach to diagnosing and controlling for method variance," (December 5, 2011). *ICIS 2011 Proceedings.* Paper 8.

Saad, G. 2011. "The Missing Link: The Biological Roots of the Business Sciences," In *Evolutionary Psychology in the Business Sciences* (pp. 1-16). Springer Berlin Heidelberg. *Evolutionary.*

Sanchez, R. J., Truxillo, D. M., and Bauer, T. N. 2000. "Development and examination of an expectancy-based measure of test-taking motivation," *Journal of Applied Psychology* (85:5), p 739.

Sasse, M. A., Brostoff, S., and Weirich, D. 2001. "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal* (19:3), pp 122-131.

Scheier, M. F., and Carver, C. S. 1985. "Optimism, coping, and health: Assessment and implications of generalized outcome expectancies," *Health psychology* (4:3), p 219.

Seligman, M., and Csikszentmihalyi, M. 2000. "Positive psychology: An introduction," *American Psychologist* (55:1), p 5.

Shaw, E., Ruby, K. G., and Post, J. M. 1998. "The Insider Threat to Information Systems: The psychology of the dangerous insider. *Security Awareness Bulletin,* 2-98, 1-10.

Sheldon, K. M., and King, L. 2001. "Why positive psychology is necessary," *American psychologist* (56:3), p 216.

Siponen, M. 2000. "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security* (8:1), pp 31-41.

Siponen, M., Pahnila, S., and Mahmood, A. 2006. "Factors influencing protection motivation and IS security policy compliance," In Proceedings of Innovations in Information Technology (pp. 1-5) IEEE.

Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS quarterly* (34:3), p 487.

Smith, C. A., and Lazarus, R. S. 1990. "Emotion and adaptation," In L.A. Pervin (ed.) *Handbook of personality: Theory and research* (pp. 609-637). New York, NY: Guilford Press.

Smith, W. K., and Lewis, M. W. 2011. "Toward a theory of paradox: A dynamic equilibrium model of organizing," *Academy of management review* (36:2), pp 381-403.

Snyder, C. R., Harris, C., Anderson, J. R., Holleran, S. A., Irving, L. M., Sigmon, S. T., Yoshinobu, L., Gibb, J., Langelle, C., and Harney, P. 1991. "The will and the ways: Development and validation of an individual-differences measure of hope," *Journal of personality and social psychology* (60:4), p 570.

Snyder, C. R., Sympson, S. C., Ybasco, F. C., Borders, T. F., Babyak, M. A., and Higgins, R. L. 1996. "Development and validation of the State Hope Scale," *Journal of personality and social psychology* (70:2), p 321.

Solomon, R. C. 2008. "The philosophy of emotions," In M. Lewis et al. (Eds) *Handbook of emotions (3rd Ed.* pp 3-15) New York, NY: Guilford Press.

Stajkovic, A. D., and Luthans, F. 1998. "Social Cognitive Theory and Self-Efficacy: Going Beyond Traditional Motivational and Behavioral Approaches," *Organizational Dynamics* (26:4), pp 62-73.

Stanton, J. M., and Stam, K. R. 2006a. *The visible employee: using workplace monitoring and surveillance to protect information assets--without compromising employee privacy or trust.* Medford, NJ: Information Today, Inc.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of end user security behaviors," *Computers & Security* (24:2), pp 124-133.

Stanton, J. M., Stam, K. R., Mastrangelo, P. M., and Jolton, J. A. 2006b. "Behavioral Information Security," *Human-Computer Interaction and Management Information Systems: Foundations* (pp 262-280). Amonk, NY: Sharpe.

Straub, D. 1989. "Validating instruments in MIS research," *MIS quarterly* (13:2), pp 147-169.

Straub, D., Boudreau, M. C., and Gefen, D. 2004. "Validation guidelines for IS positivist research," *Communications of the Association for Information Systems* (13:24), pp 380-427.

Straub, D., and Nance, W. 1990. "Discovering and disciplining computer abuse in organizations: a field study," *MIS Quarterly* (14:1), pp 45-60.

Straub, D., and Welke, R. J. 1998. "Coping with systems risk: security planning models for management decision making," *Management Information Systems Quarterly* (22:4), pp 441-470.

Symantec 2012. "2012 State of Mobility Survey."

Taylor, S., and Todd, P. A. 1995. "Understanding information technology usage: A test of competing models," *Information systems research* (6:2), pp 144-176.

Van Eerde, W., and Thierry, H. 1996. "Vroom's expectancy models and work-related criteria: A meta-analysis," *Journal of Applied Psychology* (81), pp 575-586.

Venkatesh, V. 1999. "Creation of favorable user perceptions: exploring the role of intrinsic motivation," *MIS Quarterly* (23:2), pp 239-260.

Venkatesh, V. 2000. "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information systems research* (11:4), pp 342-365.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User acceptance of information technology: Toward a unified view," *MIS quarterly* (27:3), pp 425-478.

Vroom, C., and Von Solms, R. 2004. "Towards information security behavioural compliance," *Computers & Security* (23:3), pp 191-198.

Vroom, V. 1964. "Work and motivation." Oxford, England: Wiley.

Wagnild, G. 2009. "A review of the Resilience Scale," *Journal of nursing measurement* (17:2), pp 105-113.

Wagnild, G. M., and Young, H. M. 1993. "Development and psychometric evaluation of the Resilience Scale," *Journal of Nursing Measurement* (1:2), pp 165-178.

Walumbwa, F. O., Luthans, F., Avey, J. B., and Oke, A. 2011. "Authentically leading groups: The mediating role of collective psychological capital and trust," *Journal of Organizational Behavior* (32:1), pp 4-24.

Wang, Y., Liu, L., Wang, J., and Wang, L. 2012. "Work-family Conflict and Burnout among Chinese Doctors: The Mediating Role of Psychological Capital," *Journal of occupational health* (54:3), p 232.

Watson, D., Clark, L. A., and Tellegen, A. 1988. "Development and validation of brief measures of positive and negative affect: the PANAS scales," *Journal of personality and social psychology* (54:6), p 1063.

Whitman, M. E. 2003. "Enemy at the gate: threats to information security," *Communications of the ACM* (46:8), pp 91-95.

Wiener, N. 1948. "Cybernetics; or control and communication in the animal and the machine," Oxford, England: John Wiley.

Williams, L. J., and Anderson, S. E. 1991. "Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors," *Journal of Management* (17:3), pp 601-617.

Williams, L. J., Hartman, N., and Cavazotte, F. 2010. "Method variance and marker variables: A review and comprehensive CFA marker technique," *Organizational Research Methods* (13:3), pp 477-514.

Willison, R., and Siponen, M. 2009. "Overcoming the insider: reducing employee computer crime through Situational Crime Prevention," *Communications of the ACM* (52:9), pp 133-137.

Wilson, E. 2013. "Bring your own device? Still the company's responsibility," in *The Guardian.*

Woon, I., Tan, G. W., and Low, R. Year. "A protection motivation theory approach to home wireless security," 2005, pp. 367-380.

Workman, M., Bommer, W. H., and Straub, D. 2008. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24:6), pp 2799-2816.

Wu, Z., Steward, M. D., and Hartley, J. L. 2010. "Wearing many hats: Supply managers' behavioral complexity and its impact on supplier relationships," *Journal of Business Research* (63:8), pp 817-823.

Zafar, H., and Clark, J. G. 2009. "Current State of Information Security Research In IS," *Communications of the Association for Information Systems* (24:1), pp 557-596.

Zickuhr, K., and Smith, A. 2012. "Digital differences," Pew Research Center.

Zuckerman, M. 1983. "The distinction between trait and state scales is not arbitrary: Comment on Allen and Potkay's," *Journal of personality and social psychology* (44:5), pp 1083-1086.

APPENDIX A

HUMAN USE APPROVAL FORM

LOUISIANA TECH
UNIVERSITY

MEMORANDUM

OFFICE OF UNIVERSITY RESEARCH

TO: Mr. A. J. Burns and Dr. Tom Roberts

FROM: Barbara Talbot, University Research

SUBJECT: HUMAN USE COMMITTEE REVIEW

DATE: September 24, 2012

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

"The Impact of Organizational Insiders' Psychological Capital on Protection-Motivated Behaviors"

HUC 1009

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. ***This approval was finalized on September 24, 2012 and this project will need to receive a continuation review by the IRB if the project, including data analysis, continues beyond September 24, 2013.*** Any discrepancies in procedure or changes that have been made including approved changes should be noted in the review application. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of University Research.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researchers responsibility to notify the Office of Research or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

If you have any questions, please contact Dr. Mary Livingston at 257-4315.